acquistinretepa

Reti Locali 7

Tutti i Lotti

ALLEGATO 2 ALLA GUIDA ALLA CONVENZIONE – APPARATI ATTIVI

Ultimo aggiornamento: 22/10/2021

SOMMARIO

1. DESCRIZIONE DELLA RETE PASSIVA ..... ERRORE. IL SEGNALIBRO NON È DEFINITO.

2. SWITCH 7

2.1. SWITCH TIPO 1 7

2.1.1. JUNIPER - EX2300-24T-VC 7

2.1.2. ALE OS6350-24C 8

2.1.3. HPE ARUBA - 2930F 24G 4SFP (JL259AC) 8

2.1.4. HUAWEI S5720-28P-LI-AC 10

2.1.5. ZTE 5260-28TD-H 11

2.2. SWITCH TIPO 2 12

2.2.1. JUNIPER EX2300-24P-VC 12

2.2.2. ALE OS6350-P24C 13

2.2.3. HPE 2930F 24G POE+ 4SFP SWITCH (JL261AC) 13

2.2.4. HUAWEI S5720-28P-PWR-LI-AC 15

2.2.5. ZTE 5260-28PD-H 15

2.3. SWITCH TIPO 3 16

2.3.1. JUNIPER EX3400-48T 16

2.3.2. ALE OS6560-48X4C 18

2.3.3. HPE ARUBA 2930M 48G (JL321AC) 19

2.3.4. HUAWEI S5730-68C-SI-AC 20

2.3.5. ZTE 5950-60TM 20

2.4. SWITCH TIPO 4 21

2.4.1. JUNIPER EX3400-48P 21
2.4.2. ALE OS6560-P48X4C 23
2.4.3. HPE ARUBA 2930M 48G POE+ SWITCH (JL322AC) 24
2.4.4. HUAWEI S5730-68C-PWR-SI-AC 25
2.4.5. ZTE 5950-60PM 25
2.5. SWITCH TIPO 5 27
2.5.1. JUNIPER EX4300-48MP 27
2.5.2. ALE OS6860N-P48MZC 28
2.5.3. HPE ARUBA – 2930M 40 G 8SR (R0M67AC) 28
2.5.4. HUAWEI S6720-56C-PWH-SI-AC 30
2.5.5. ZTE 5950-54PM-H-C 30
2.6. SWITCH TIPO 6 31
2.6.1. JUNIPER EX4300-48P 31
2.6.2. ALE OS6860-P48C 32
2.6.3. HPE ARUBA 3810M 48G POE+ 4SFP+ (JL429AC) 32
2.6.4. HUAWEI S5730-60C-PWH-HI 35
2.6.5. ZTE 5950-56PM-H 35
2.7. SWITCH TIPO 7 35
2.7.1. JUNIPER EX4300-32F 35
2.7.2. ALE OS6860E-U28C 37
2.7.3. HPE ARUBA 5510 24G SFP 4SFP+ HI (JH149AC) 38
2.7.4. HUAWEI S5730-44C-HI-24S 40

2.7.5. ZTE 5960-32DL 40
2.8. SWITCH TIPO 8 41
2.8.1. JUNIPER EX4600-40F-AFO 41
2.8.2. ALE OS6900-X72-FC 42
2.8.3. HPE ARUBA FF 5940 2-SLOT (JH397AC) 43
2.8.4. HUAWEI S6720-54C-EI-48S-AC 43
2.8.5. ZTE 5960-64DL-H 43
2.9. SWITCH TIPO 9 44
2.9.1. JUNIPER EX9204-RED3B-AC 44
2.9.2. ALE OS9907-RCB-A 45
2.9.3. HPE ARUBA 5412R ZL (J9822A) 46
2.9.4. HUAWEI 7706 49
2.9.5. ZTE 8905E-CMP3A-AC2 50
2.10. SWITCH TIPO 10 51
2.10.1. JUNIPER JUNOS SPACE NETWORK DIRECTOR 51
2.10.2. ALE OMNIVISTA 2500 52
2.10.3. HPE ARUBA – AIRWAVE (AW-100C - AW-500C - AW-1000C) 57
2.10.4. HUAWEI ESIGHT 67
2.10.5. ZTE NETNUMEN U31 R22 70
3. PRODOTTI PER L'ACCESSO WIRELESS 70
3.1. ACCESS POINT PER AMBIENTI INTERNI 70
3.1.1. HUAWEI AP4051DN 70

3.1.2. ALE AP1201-RWC 70
3.1.3. HPE R0G68AC 71
3.2. ACCESS POINT PER AMBIENTI ESTERNI 80
3.2.1. HUAWEI AP8150DN 80
3.2.2. ALE AP1251-RWC 80
3.2.3. HPE JZ162AC 81
3.3. DISPOSITIVO DI GESTIONE DEGLI ACCESS POINT 88
3.3.1. HUAWEI AC6508 88
3.3.2. ALE AP1221-RWC 90
3.3.3. HPE Q9H62AFS-C 91
4. DISPOSITIVI PER LA SICUREZZA DELLE RETI 101
4.1. DISPOSITIVI DI SICUREZZA FASCIA BASE 101
4.1.1. HUAWEI USG6515E 101
4.1.2. FORTINET FG-60E-BDL-950-12 103
4.1.3. CHECKPOINT CPAP-SG750-NGTP 103
4.2. DISPOSITIVI DI SICUREZZA FASCIA MEDIA 103
4.2.1. HUAWEI USG6620-C 103
4.2.2. FORTINET FG-200E-BDL-950-12 103
4.2.3. CHECKPOINT CPAP-SG5400-NGTP 108
4.3. DISPOSITIVI DI SICUREZZA FASCIA ALTA 108
4.3.1. HUAWEI USG6630E 108
4.3.2. FORTINET FG-500E-BDL-950-12 110

4.3.3. CHECKPOINT CPAP-SG5800-NGTP-HPP 110
4.4. DISPOSITIVI DI SICUREZZA FASCIA TOP 111
4.4.1. HUAWEI USG6680E 111
4.4.2. FORTINET FG-1500D-BDL-950-12 112
4.4.3. CHECKPOINT CPAP-SG15400-NGTP-HPPVS10 112
4.5. DISPOSITIVI DI SICUREZZA FASCIA ENTERPRISE 113
4.5.1. HUAWEI USG6680E 113
4.5.2. FORTINET FG-3100D-BDL-C 114
4.5.3. CHECKPOINT CPAP-SG23500-NGTP-HPP 119
4.6. DISPOSITIVI DI SICUREZZA SANDBOX 119
4.6.1. HUAWEI FIREHUNTER6300 119
4.6.2. FORTINET FSA-1000F-BDL-C 120
4.7. NETWORK ACCESS CONTROL 124
4.7.1. HPE JZ508A 124
4.7.2. FORESCOUT 135
4.8. SECURITY E-MAIL GATEWAY 146
4.8.1. FORTINET 146
4.8.2. SONICWALL 150
5. GRUPPI DI CONTINUITÀ 158
6. PIATTAFORMA DI GESTIONE E MONITORAGGIO DELLA RETE 162

1. Premessa

Questo documento contiene la descrizione di dettaglio di tutti gli apparati attivi presenti nella convenzione: switch, dispositivi e servizi di sicurezza ed apparati wireless. Sono descritti, inoltre, in dettaglio anche gli UPS e il sistema di gestione.

2. Switch

Si riporta quanto proposto da Vodafone Italia per gli apparati attivi switch. Nello specifico si propongono 50 diversi apparati per un totale di 5 diversi Brand: Juniper, ALE, HPE, Huawei e ZTE.

2.1. Switch Tipo 1

2.1.1. Juniper - EX2300-24T-VC

Gli switch ethernet della serie EX2300 sono apparati compatti ed efficienti, ideali per il livello di accesso in ambito branch, retail e campus. Sono switch "cloud-ready" e abilitati per l'installazione zero-touch (ZTP) senza configurazione manuale, tramite il servizio di **Wired Assurance**. Gli switch supportano la tecnologia **Virtual Chassis** ed è possibile connettere e gestire fino a 4 switch EX2300 tra loro, come se fossero in singolo apparato logico.

Funzionalità in evidenza:

Porte	24x1GbE e 4 SFP/SFP+ 1/10Gbe
Switch capacity	176 Gbps
Fabric	Virtual Chassis

Virtual Chassis

La tecnologia Virtual Chassis permette di collegare fino a 4 EX2300 e di gestirli come un solo device e riduce i costi operativi, semplificando la gestione.

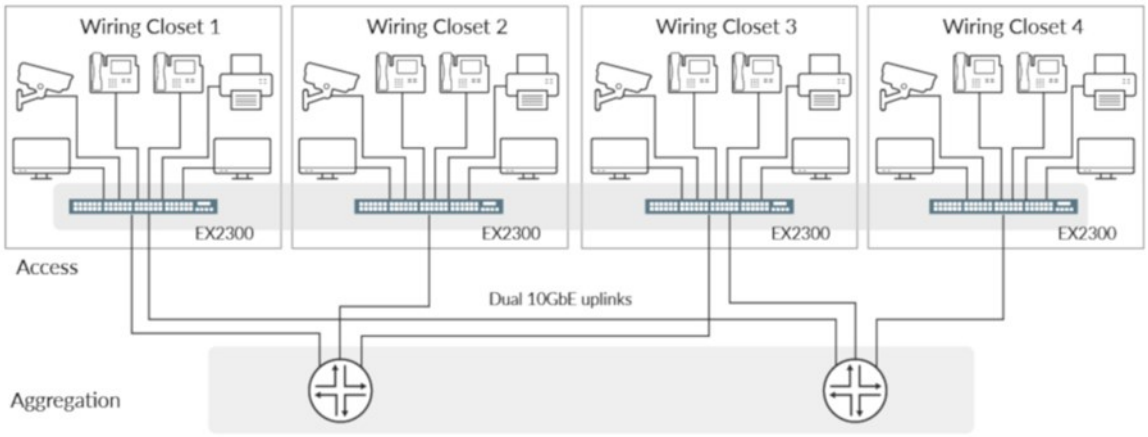


Figure 1: EX2300 switches support Virtual Chassis technology, which enables up to four interconnected switches to operate as a single, logical device.

La configurazione in Virtual Chassis garantisce alta affidabilità e semplifica il disegno della rete.

QoS con 8 code di priorità

Lo switch ha 8 code per porta che assicurano la gestione della priorità del traffico voce, video e di molteplici classi di traffico dati e permettendo, ad esempio, la gestione della QoS per reti dedicata alla building automation o ai sistemi di video sorveglianza.

2.1.2. ALE OS6350-24C

In fase di sostituzione per End of Sale

2.1.3. HPE Aruba - 2930F 24G 4SFP (JL259AC)

Gli Aruba 2930F appartenenti alla tipologia 1 in convenzione Consip Lan 7 sono switch wire-speed, Layer 3, adatti ad offrire alle Amministrazioni un network dalla massima sicurezza e "high intelligence". Lo switch (da rack standard 19") dispone di 24 porte autosensing 10/100/1000 Base-T, di 4 porte 1GbE SFP. In aggiunta dispone di una porta seriale e di una porta USB micro-B per la gestione locale.

La banda della matrice di switching è pari a 56 Gbps (rispettando la banda minima richiesta di 48 Gbps) e il throughput aggregato è tale da garantire prestazioni wire-speed su tutte le porte.

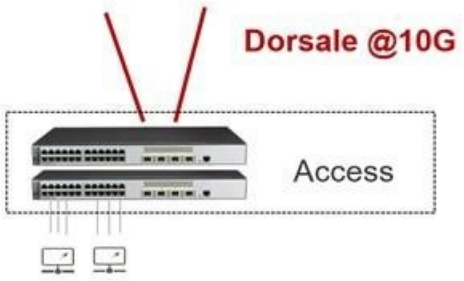
Le funzionalità Layer 3 includo fino a 256 Static IP routing e 10.000 rotte con il protocollo RIPv1, RIPv2 e RIPng. Viene supportato il protocollo OSPF su singola area e fino a 8 interfaccie di routing. Supporto Policy-based routing.

- QoS: supporta le seguenti azioni anticongestione: impostazione del tag di priorità IEEE 802.1p basato su indirizzo IP, IP Type of Service (ToS), protocollo L3, port number TCP/UDP, porta sorgente e DiffServ, accodamento Strict Priority (SP), Egress Queue Rate-limiting, Guaranteed Bandwidth Minimums, Port e Priority-based Rate Limiting, Selectable Queuing Configurations.
- Controllo del traffico broadcast: consente la limitazione della velocità del traffico in broadcast per ridurre il traffico di rete indesiderato;
- Semplifica il nome delle porte: assegnazione di nomi descrittivi alle porte;
- Configurazione e gestione in modalità remota: disponibile tramite browser Web sicuro o interfaccia a linea di comando (CLI);
- Privilegi di livello responsabile e operatore: consentono l'accesso in sola lettura (operatore) o lettura e scrittura (manager) alle interfacce CLI e di gestione di browser Web;
- Autorizzazione di comandi: utilizza RADIUS per il collegamento di un elenco personalizzato di comandi CLI al login di un singolo amministratore di rete;
- Auto-MDIX: adeguamento automatico per cavi dritti o crossover su tutte le porte 10/100 e 10/100/1000;
- Controllo di flusso: mediante lo standard IEEE 802.3x, permette di ridurre la congestione in situazioni di traffico intenso;
- Uplink Gigabit: porte per connettività 1Gb SFP;
- ACL (access control list) in wire-speed basate su hardware: implementazione di ACL ricche di funzionalità per garantire elevati livelli di sicurezza e facilità di amministrazione senza impatto sulle prestazioni di rete;
- Local user role definisce un set di politiche di accesso allo switch come sicurezza, di autenticazione e QoS. Uno User Role può essere applicato a gruppi di utenti o switch. L'applicazione del roulo può avvenire mediante la configurazione dell'apparato o utilizzando il Policy Manager ClearPass;
- Per-port tunneled node; fornisce un tunnel sicuro per il trasporto del traffico di rete di una porta dello switch verso un Controller Aruba. Le politiche di accesso verranno applicate dal controller;
- Spanning Tree/MSTP, RSTP: protocolli per link ridondanti e prevenzione dei loop di rete;
- Port trunking: fornisce livelli superiori di throughput da switch a switch e ridondanza a livello di collegamento, con supporto per aggregazione di collegamenti basati su standard (IEEE 802.3ad); supporta fino a 128 trunk, con max 8 collegamenti (porte) per ciascun trunk;
- 32.768 MAC address: forniscono l'accesso a molti dispositivi Layer 2;
- Supporto e tagging VLAN: supporta IEEE 802.1Q, con 4094 ID VLAN simultanei; supporta VLAN basate su porta, su MAC e su protocollo;

- Supporto della tecnologia di overlay VxLAN ;
- ARP: determina il MAC address di un altro host IP nella stessa sottorete;
- Dynamic Host Configuration Protocol (DHCP): semplifica la gestione di reti IP di grandi dimensioni e supporta client e server;
- GUI Web protetta: offre interfaccia grafica sicura di facile utilizzo per la configurazione del modulo mediante HTTPS;
- Gli switch della serie Aruba 2930F supportano Simple Network Management Protocol (SNMP) v1/v2c/v3 e possono essere gestiti da Aruba Airwave. Supportano anche command-line interface (CLI), Web network management e Telnet per facilitare la gestione del sistema;
- La tecnologia di clustering VSF permette all'amministratore di rete configurare un Virtual Chassis che include fino ad 8 apparati della serie Aruba 2930F. VSF permette la gestione di un unico switch di comando con un unico indirizzo IP, riducendo così il numero di indirizzi IP e rendendo più efficiente la gestione del network. La tecnologia VSF permette di configurare canali aggregati LACP tra apparati diversi inclusi nello stesso Virtual Chassis riducendo la necessità di protocolli di ridondanza come Spanning Tree e VRRP.

2.1.4. Huawei S5720-28P-LI-AC

Il modello Ethernet Switch S5720-28P-LI-AC fa parte della series S5720LI. È uno switch Layer 3 con supporto di routing statico, RIP e OSPF. Installabile a rack 19", equipaggia 24 porte 10/100/1000 Ethernet su rame e 4 porte 1G ottico su SFP, che possono essere oggetto di upgrade a 10G SFP+ o essere utilizate come interfacce GPON con opportuno transceiver. In dotazione è fornito un cavo di stack da 1 metro da usare su una delle 4 porte ottiche e con cui è possibile metterlo in stack con i modelli della stessa series LI (tra cui il Tipo 2 PoE della presente Convenzione).



L'apparato ha una matrice di switching non blocking con inoltro del traffico in modalità wirespeed e capacità di processamento pacchetti pari a 51Mpps (milioni di pacchetti per secondo).

I modelli della famiglia LI possono implementare, di concerto ai modelli di Tipo 7, 8 e 9, il concetto di Super Virtual Fabric in cui Aggregazione e switch di Accesso (e Wi-Fi Access Point) sono visti come un unico switch

logico semplificando il management della rete, la configurazione e il monitoraggio dei servizi dall'elemento di Aggregazione e permettendo di dispiegare gli switch di accesso in modalità plug-and-play.

È gestibile dal sistema di management eSight (Tipo 10) incluso all'interno della Convenzione.

2.1.5. ZTE 5260-28TD-H

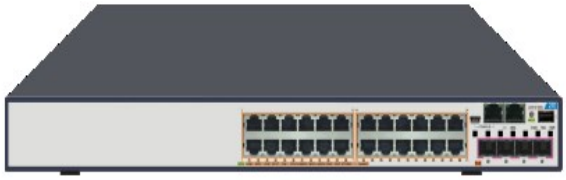
La famiglia di switch ZXR10 5260-H (1 RU) si compone di apparati installabili a rack 19", gigabit ethernet L3, con funzionalità stackable, ideali per le reti di accesso ed aggregazione, che forniscono fino a 28 interfacce (24*GE + 4*10GE), 1 GE MNG, 1RJ45 Console and 1 Mini USB Console, 1 ventola di raffreddamento e singola alimentazione. Gli switch della serie ZXR10 5260-H supportano le seguenti ulteriori funzionalità:

- VSC (Virtual Switch Cluster) 2.0: Fino a 4 apparati sono visti, logicamente, come un unico apparato;
- ZESR – ZTE Ethernet Smart Ring network technology: algoritmo di protezione di un anello in fibra in 10ms;
- Flexible PoE: protezione dalle sovratensioni e possibilità di schedulare l'alimentazione per fasce orarie;
- Zero-touch provisioning: caricamento della prima configurazione tramite Stick USB;
- M-Button: Spie di segnalazione guasti sul fronte dell'apparato.

Il modello proposto è 5260-28TD-H (Ethernet 10/100/1000 con uplink a 10Gb).

L'apparato comprende: 24 porte Ethernet 10/100 /1000M RJ45, 4 porte ottiche 10GE SFP+ e 1 modulo di alimentazione AC. La capacità di switching è di 128 Gbps.

L'apparato è gestibile dal sistema di management NetNumen, incluso all'interno della Convenzione (Tipo 10).



2.2. Switch Tipo 2

2.2.1. Juniper EX2300-24P-VC

Gli switch ethernet della serie EX2300 sono apparati compatti ed efficienti, ideali per il livello di accesso in ambito branch, retail e campus. Sono switch "cloud-ready" e abilitati per l'installazione zero-touch (ZTP) senza configurazione manuale, tramite il servizio di **Wired Assurance**. Gli switch supportano la tecnologia **Virtual Chassis** ed è possibile connettere e gestire fino a 4 switch EX2300 tra loro, come se fossero in singolo apparato logico.

Funzionalità in evidenza

Porte	24x1GbE e 4 SFP/SFP+ 1/10Gbe
Power	Poe/PoE+ fino a 30W per porta
Switch capacity	176 Gbps
Fabric	Virtual Chassis

Virtual Chassis

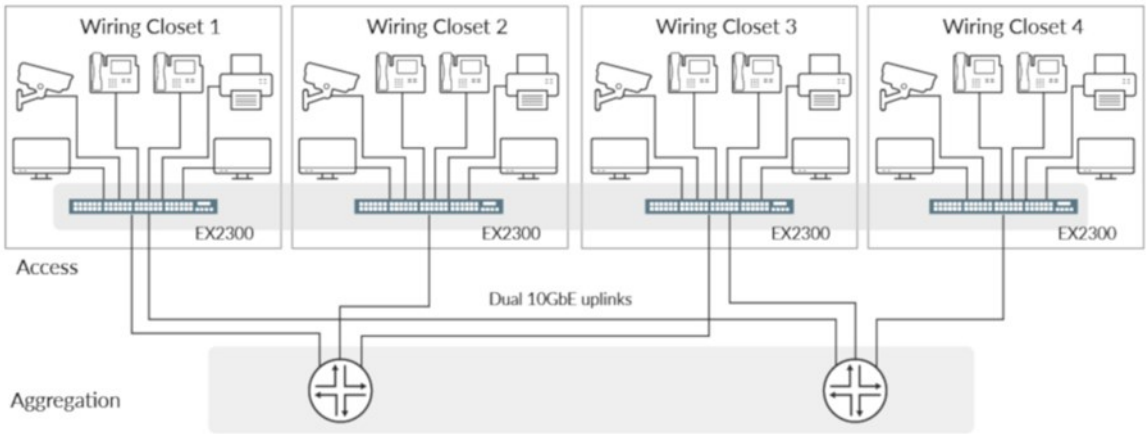


Figure 1: EX2300 switches support Virtual Chassis technology, which enables up to four interconnected switches to operate as a single, logical device.

La tecnologia Virtual Chassis permette di collegare fino a 4 EX2300 e di gestirli come un solo device e riduce i costi operativi, semplificando la gestione. La configurazione in Virtual Chassis garantisce alta affidabilità e semplifica il disegno della rete.

QoS con 8 code di priorità

Lo switch ha 8 code per porta che assicurano la gestione della priorità del traffico voce, video e di molteplici classi di traffico dati e permettendo, ad esempio, la gestione della QoS per reti dedicata al building automation o ai sistemi di video sorveglianza.

2.2.2. ALE OS6350-P24C

In fase di sostituzione per End of Sale

2.2.3. HPE 2930F 24G PoE+ 4SFP Switch (JL261AC)

Gli Aruba 2930F appartenenti alla tipologia 2 in convenzione Consip Lan 7 sono switch wire-speed, Layer 3, adatti ad offrire alle Amministrazioni un network dalla massima sicurezza e "high intelligence". Lo switch (da rack standard 19") dispone di 24 porte autosensing 10/100/1000 Base-T PoE+, di 4 porte 1GbE SFP. In aggiunta dispone di una porta seriale e di una porta USB micro-B per la gestione locale.

La banda della matrice di switching è pari a 56 Gbps (rispettando la banda minima richiesta di 48 Gbps) e il throughput aggregato è tale da garantire prestazioni wire-speed su tutte le porte.

Le funzionalità Layer 3 includo fino a 256 Static IP routing e 10.000 rotte con il protocollo RIPv1, RIPv2 e RIPng. Viene supportato il protocollo OSPF su singola area e fino a 8 interfaccie di routing. Supporto Policy-based routing.

- QoS: supporta le seguenti azioni anticongestione: impostazione del tag di priorità IEEE 802.1p basato su indirizzo IP, IP Type of Service (ToS), protocollo L3, port number TCP/UDP, porta sorgente e DiffServ, accodamento Strict Priority (SP), Egress Queue Rate-limiting, Guaranteed Bandwidth Minimums, Port e Priority-based Rate Limiting, Selectable Queuing Configurations;
- Controllo del traffico broadcast: consente la limitazione della velocità del traffico in broadcast per ridurre il traffico di rete indesiderato;
- Semplifica il nome delle porte: assegnazione di nomi descrittivi alle porte;
- Configurazione e gestione in modalità remota: disponibile tramite browser Web sicuro o interfaccia a linea di comando (CLI);
- Privilegi di livello responsabile e operatore: consentono l'accesso in sola lettura (operatore) o lettura e scrittura (manager) alle interfacce CLI e di gestione di browser Web;
- Autorizzazione di comandi: utilizza RADIUS per il collegamento di un elenco personalizzato di comandi CLI al login di un singolo amministratore di rete;

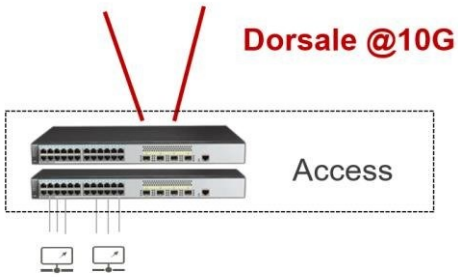
- Auto-MDIX: adeguamento automatico per cavi dritti o crossover su tutte le porte 10/100 e 10/100/1000;
- Controllo di flusso: mediante lo standard IEEE 802.3x, permette di ridurre la congestione in situazioni di traffico intenso;
- Uplink Gigabit: porte per connettività 1Gb SFP;
- ACL (access control list) in wire-speed basate su hardware: implementazione di ACL ricche di funzionalità per garantire elevati livelli di sicurezza e facilità di amministrazione senza impatto sulle prestazioni di rete;
- Local user role definisce un set di politiche di accesso allo switch come sicurezza, di autenticazione e QoS. Uno User Role può essere applicato a gruppi di utenti o switch. L'applicazione del roulo può avvenire mediante la configurazione dell'apparato o utilizzando il Policy Manager ClearPass;
- Per-port tunneled node; fornisce un tunnel sicuro per il trasporto del traffico di rete di una porta dello switch verso un Controller Aruba. Le politiche di accesso verranno applicate dal controller;
- Spanning Tree/MSTP, RSTP: protocolli per link ridondanti e prevenzione dei loop di rete;
- Port trunking: fornisce livelli superiori di throughput da switch a switch e ridondanza a livello di collegamento, con supporto per aggregazione di collegamenti basati su standard (IEEE 802.3ad); supporta fino a 128 trunk, con max 8 collegamenti (porte) per ciascun trunk;
- 32.768 MAC address: forniscono l'accesso a molti dispositivi Layer 2;
- Supporto e tagging VLAN: supporta IEEE 802.1Q, con 4094 ID VLAN simultanei; supporta VLAN basate su porta, su MAC e su protocollo;
- Supporto della tecnologia di overlay VxLAN;
- ARP: determina il MAC address di un altro host IP nella stessa sottorete;
- Dynamic Host Configuration Protocol (DHCP): semplifica la gestione di reti IP di grandi dimensioni e supporta client e server;
- GUI Web protetta: offre interfaccia grafica sicura di facile utilizzo per la configurazione del modulo mediante HTTPS;
- Gli switch della serie Aruba 2930F supportano Simple Network Management Protocol (SNMP) v1/v2c/v3 e possono essere gestiti da Aruba Airwave. Supportano anche command-line interface (CLI), Web network management e Telnet per facilitare la gestione del sistema;
- La tecnologia di clustering VSF permette all'amministratore di rete configurare un Virtual Chassis che include fino ad 8 apparati della serie Aruba 2930F. VSF permette la gestione di un unico switch di comando con un unico indirizzo IP, riducendo così il numero di indirizzi IP e rendendo più efficiente la gestione del network. La tecnologia VSF permette di configurare canali aggregati LACP tra apparati

diversi inclusi nello stesso Virtual Chassis riducendo la necessità di protocolli di ridondanza come Spanning Tree e VRRP.

2.2.4. Huawei S5720-28P-PWR-LI-AC

Il modello Ethernet Switch S5720-28P-PWR-LI-AC fa parte della series S5720LI. È uno switch Layer 3 con supporto di routing statico, RIP e OSPF. Installabile a rack 19", equipaggia 24 porte 10/100/1000 Ethernet PoE+ su rame e 4 porte 1G ottico su SFP, che possono essere oggetto di upgrade a 10G SFP+ o essere utilizzate come interfacce GPON con opportuno transceiver.

In aggiunta dispone di una porta seriale e di una porta USB per la gestione locale. In dotazione è fornito un cavo di stack da 1 metro da usare su una delle 4 porte ottiche e con cui è possibile metterlo in stack con i modelli della stessa series LI (tra cui il Tipo 1 della presente Convenzione).



L'apparato ha una matrice di switching non blocking con inoltro del traffico in modalità wirespeed e capacità di processamento pacchetti pari a 51Mpps (milioni di pacchetti per secondo).

I modelli della famiglia LI possono implementare, di concerto ai modelli di Tipo 7, 8 e 9, il concetto di Super Virtual Fabric in cui Aggregazione e switch di Accesso (e Wi-Fi Access Point) sono visti come un unico switch logico semplificando il management della rete, la configurazione e il monitoraggio dei servizi dall'elemento di Aggregazione e permettendo di dispiegare gli switch di accesso in modalità plug-and-play.

È gestibile (configurazione, monitoraggio e allarmistica) dal sistema di management eSight (Tipo 10) incluso all'interno della Convenzione.

2.2.5. ZTE 5260-28PD-H

La famiglia di switch ZXR10 5260-H (1 RU) si compone di apparati installabili a rack 19", gigabit ethernet L3, con funzionalità stackable, ideali per le reti di accesso ed aggregazione, che forniscono fino a 28 interfacce (24*GE non-PoE/PoE/POE+ + 4*10GE), 1 GE MNG, 1RJ45 Console and 1 Mini USB Console, 1 ventola di

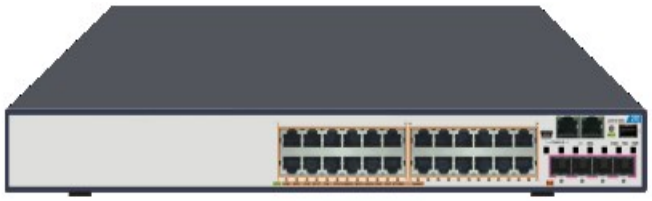
raffreddamento e doppia alimentazione. Gli switch della serie ZXR10 5260-H supportano le seguenti ulteriori funzionalità:

- VSC (Virtual Switch Cluster) 2.0: Fino a 4 apparati sono visti, logicamente, come un unico apparato;
- ZESR – ZTE Ethernet Smart Ring network technology: algoritmo di protezione di un anello in fibra in 10ms;
- Flexible PoE: protezione dalle sovratensioni e possibilità di schedulare l'alimentazione per fasce orarie;
- Zero-touch provisioning: caricamento della prima configurazione tramite Stick USB;
- M-Button: Spie di segnalazione guasti sul fronte dell'apparato.

Il modello proposto è 5260-28PD-H (Ethernet 10/100/1000 non-PoE/PoE/POE+ con uplink a 10Gb).

L'apparato comprende: 24 porte Ethernet 10/100 /1000M RJ45, 4 porte ottiche 10GE SFP+ e 2 moduli di alimentazione AC. La capacità di switching è di 128 Gbps.

L'apparato è gestibile dal sistema di management NetNumen, incluso all'interno della Convenzione (Tipo 10).



2.3. Switch Tipo 3

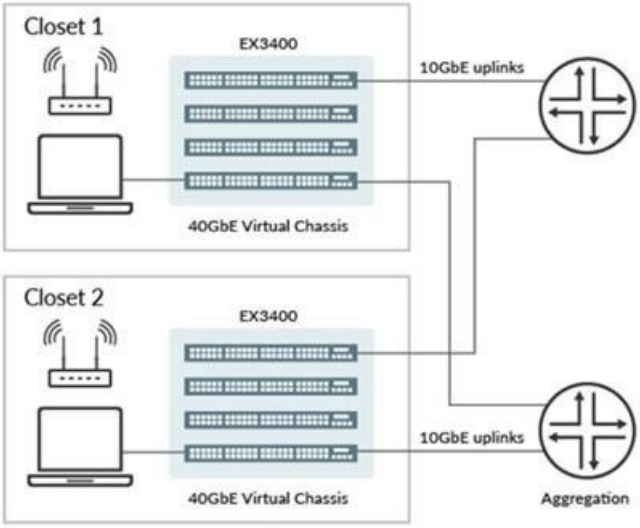
2.3.1. Juniper EX3400-48T

Gli switch ethernet della serie EX3400 sono apparati prestazionali, in grado di soddisfare i requisiti delle reti enterprise convergenti (voip, video e data), ad un costo vantaggioso. Compatti e prestazionali gli switch E3400 forniscono prestazioni di categoria superiore ed elevata affidabilità hardware e software.

Gli EX3400 sono "cloud-ready" e supportano l'installazione zero-touch (ZTP), che non richiede alcuna configurazione manuale, tramite il servizio di **Wired Assurance**. Gli switch supportano la tecnologia **Virtual Chassis** ed è possibile connettere e gestire fino a 10 switch EX4300 tra loro, come se fossero in singolo apparato logico. **Funzionalità in evidenza**

Porte	48x1GbE – 4 SFP/SFP+ 1/10Gbe – 2 QSFP+ 40Gbe

Form Factor	1RU
Power	Alimentazione ridondata
Switch capacity	336 Gbps
Fabric	Virtual Chassis fino a 10 switch



Virtual Chassis

La tecnologia Virtual Chassis permette di collegare fino a 10 EX3400 e di gestirli come un solo apparato, riducendo i costi operativi e semplificando la gestione. La configurazione in Virtual Chassis garantisce alta affidabilità e semplifica il disegno della rete.

MACsec

Gli switch EX3400 supportano IEEE 802.1ae MACsec e garantiscono la confidenzialità, integrità e autenticità della comunicazione dei dati a livello link-layer. Gli switch garantiscono 88Gbps di throughput con cifratura a livello hardware sulle porte 1/10Gbps.

QoS con 12 code di priorità

Lo switch ha 12 code, 8 unicast e 4 multicast, per porta, che assicurano la gestione della priorità del traffico voce, video e di molteplici classi di traffico dati e permettendo, ad esempio, la gestione della QoS per reti dedicata al building automation o ai sistemi di video sorveglianza.

2.3.2. ALE OS6560-48X4C

Alcatel-Lucent Enterprise OmniSwitch® 6560 è una famiglia di Switch Ethernet Stackable a configurazione fissa che forniscono accesso Gigabit Ethernet ed è una soluzione di accesso ideale per la realizzazione di reti aziendali.

Il modello in oggetto è uno Switch Layer 2 a forma compatta per inserimento in armadio a 19 pollici che fornisce 48 porte 10/100/1000BaseT, 4 porte ottiche di uplink SFP+ 10 Gbps e 2 porte di stacking (fino a 8 unità per stack) con possibilità di equipaggiare un power supply ridondato. Offre un design ottimizzato per flessibilità e scalabilità con un basso consumo energetico.

L'apparato supporta protocolli di livello 3 di base, incluso VRRP e fornisce switching capacity di 216 Gbps e wire-speed performance su tutte le porte. Incluso a corredo il cavo di stack di lunghezza 1 mt.

OmniSwitch 6560 è una soluzione completa per la realizzazione del livello di accesso nelle reti di medie e grandi dimensioni. Utilizza il collaudato Alcatel-Lucent Operating System (AOS) per fornire alta disponibilità, sicurezza, protezione ed è facilmente gestibile.

Supporta innovative soluzioni per la visibilità e la gestione dei dispositivi collegati sulle porte utente (Fingerprinting IoT), in collaborazione con il sistema di gestione OmniVista 2500 (tipo 10 in convenzione), al fine di identificare e classificare il tipo di dispositivo attestato all'apparato, e successivamente attivare delle regole di micro-segmentazione sulla base delle scelte dell'amministratore di rete.

2.3.3. HPE Aruba 2930M 48G (JL321AC)

Gli Aruba 2930M, appartenenti alla tipologia 3 in convenzione Consip Lan 7, sono switch Layer 3 Ethernet in grado di supportare diversi servizi: permettono il forwarding IPv6 e offrono alle Amministrazioni quattro porte 10-Gigabit Ethernet (GbE) e power supply ridondato interno. Gli Aruba 2930M condividono le stesse funzionalità Software descritte per gli Aruba 2930F della Tipologia 1 e tipologia 2 ad eccezione della funzionalità di Virtual Chassis.

La serie Aruba 2930M offre un accesso da 1-GbE e può essere utilizzata nel perimetro (edge) del network o per collegare i cluster dei server nei data center.

Il Virtual Chassis dei Aruba 2930M viene gestita tramite i moduli di stack Hardware.

La tecnologia brevettata Aruba Stack permette la configurazione di un Virtual Chassis di dimensione massima di dieci apparati, interconnessi tramite un modulo con due porte da 50GbE. Il modulo ed i cavi di connessione sono inclusi in bundle con ogni apparato fornito in convenzione Consip Lan 7.

- Supporto multiservizi

  Gli switch della serie Aruba 2930M supportano la tecnologia LLDP-MED (Media Endpoint Discovery), permettendo agli switch di individuare automaticamente il traffico voce e di accelerare il suo passaggio nel network. Ciò ottimizza il bandwidth per le informazioni time-sensitive e previene efficacemente l'impatto causato da bruschi flussi di dati nello streaming voce.

- Politiche di controllo sulla sicurezza globale.

  Gli switch della serie Aruba 2930M includono il supporto per l'autenticazione 802.1x e l'autenticazione centralizzata degli indirizzi MAC che controlla l'access rights degli utenti al network secondo gli indirizzi MAC e delle porte.Il supporto per Secure Shell Version 2 (SSHv2) garantisce la sicurezza delle informazioni attraverso un potente strumento di autenticazione che previene dagli attacchi al network come lo spoofing degli indirizzi IP e dall'intercettazione di password troppo semplici.

- Eccellente Gestibilità.

Gli switch della serie Aruba 2930M supportano Simple Network Management Protocol (SNMP) v1/v2c/v3 e possono essere gestiti da Aruba Airwave. Supportano anche command-line interface (CLI), Web network management e Telnet per facilitare la gestione del sistema.

Un'altra caratteristica di gestione degli switch della serie Aruba 2930M è di permettere a una rete VLANs di essere classificata nei propri indirizzi MAC, ciò offre all'Amministrazione una gestione intelligente e flessibile delle risorse mobile office in collaborazione con le policy ACL basate su VLANs globali, ottimizzando le risorse hardware e, allo stesso tempo, semplificando la configurazione degli utenti.

- HPE Redundant Power Systems

  Gli switch Aruba 2930M forniscono la possibilità di ridondare internamente l'alimentazione. In convenzione sono presenti, come elementi opzionali, i corrispondenti alimentatori di backup. In particolare, per la tipologia 3 è disponibile il Power Supply X371 12VDC 250W. Per migliorare l'efficienza ed il risparmio energetico, i power supply sono certificati 80 PLUS Gold and Platinum. Il supporto dello standard IEEE 802.3az Energy-efficient Ethernet (EEE) riduce il consumo energetico durante i periodi di inattività.

2.3.4. Huawei S5730-68C-SI-AC

In fase di sostituzione per End of Sale

2.3.5. ZTE 5950-60TM

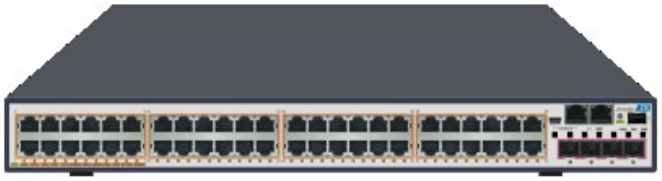
La famiglia di switch ZXR10 5950 (1 RU) si compone di apparati installabili a rack 19", gigabit ethernet L3, con funzionalità stackable, ideali per le reti di accesso ed aggregazione. Il prodotto offerto fornisce fino a 52 interfacce (48*GE + 4*10GE), 1 Slot di espansione, 1 GE MNG, 1 RJ45 Console, 1 Mini USB Console, 1 ventola di raffreddamento e doppia alimentazione. Gli switch della serie ZXR10 5950 supportano le seguenti ulteriori funzionalità:

- VSC (Virtual Switch Cluster) 2.0: Fino a 4 apparati sono visti, logicamente, come un unico apparato;
- ZESR – ZTE Ethernet Smart Ring network technology: algoritmo di protezione di un anello in fibra in 10ms;
- Flexible PoE: protezione dalle sovratensioni e possibilità di schedulare l'alimentazione per fasce orarie;
- Zero-touch provisioning: caricamento della prima configurazione tramite Stick USB;
- M-Button: Spie di segnalazione guasti sul fronte dell'apparato.

Il modello proposto è 5950-60PM (Ethernet 10/100/1000 con uplink a 10Gb).

L'apparato comprende: 48 porte Ethernet 10/100/1000M RJ45, 4 porte ottiche 10GE SFP+ e 2 moduli di alimentazione AC. La capacità di switching è di 336 Gbps.

L'apparato è gestibile dal sistema di management NetNumen, incluso all'interno della Convenzione (Tipo 10).



2.4. Switch Tipo 4

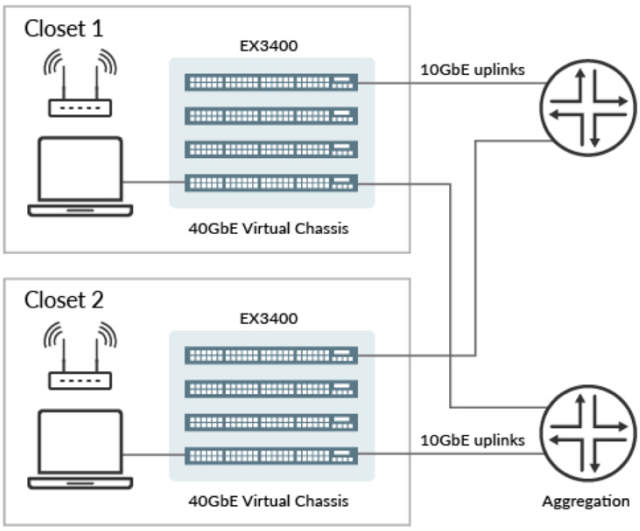
2.4.1. Juniper EX3400-48P

Gli switch ethernet della serie EX3400 sono apparati prestazionali, in grado di soddisfare i requisiti delle reti enterprise convergenti (voip, video e data), ad un costo vantaggioso. Compatti e prestazionali gli switch E3400 forniscono prestazioni di categoria superiore ed elevata affidabilità hardware e software.

Gli EX3400 sono "cloud-ready" e supportano l'installazione zero-touch (ZTP), che non richiede alcuna configurazione manuale, tramite il servizio di **Wired Assurance**. Gli switch supportano la tecnologia **Virtual Chassis** ed è possibile connettere e gestire fino a 10 switch EX4300 tra loro, come se fossero in singolo apparato logico.

Funzionalità in evidenza

Porte	48x1GbE – 4 SFP/SFP+ 1/10Gbe – 2 QSFP+ 40Gbe
Power	PSU ridondata, PoE/PoE+ fino a 30W per porta
Switch capacity	336 Gbps
Fabric	Virtual Chassis fino a 10 switch



Virtual Chassis

La tecnologia Virtual Chassis permette di collegare fino a 10 EX3400 e di gestirli come un solo apparato, riducendo i costi operativi e semplificando la gestione. La configurazione in Virtual Chassis garantisce alta affidabilità e semplifica il disegno della rete.

MACsec

Gli switch EX3400 supportano IEEE 802.1ae MACsec e garantiscono la confidenzialità, integrità e autenticità della comunicazione dei dati a livello link-layer. Gli switch garantiscono 88Gbps di throughput con cifratura a livello hardeware sulle porte 1/10Gbps.

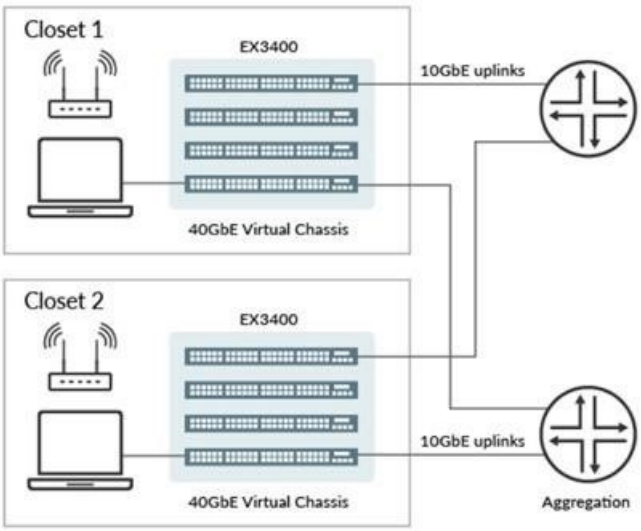


Figure 1: EX3400 Virtual Chassis deployments

QoS con 12 code di priorità

Lo switch ha 12 code, 8 unicast e 4 multicast, per porta, che assicurano la gestione della priorità del traffico voce, video e di molteplici classi di traffico dati e permetteno, ad esempio, la gestione della QoS per reti dedicata al building automation o ai sistemi di video sorveglianza.

2.4.2. ALE OS6560-P48X4C

Alcatel-Lucent Enterprise OmniSwitch® 6560 è una famiglia di Switch Ethernet Stackable a configurazione fissa che forniscono accesso Gigabit Ethernet ed è una soluzione di accesso ideale per la realizzazione di reti aziendali.

Il modello in oggetto è uno Switch Layer 2 a forma compatta per inserimento in armadio a 19 pollici che fornisce 48 porte 10/100/1000BaseT PoE (supporto degli standard 802.3af e 802.3at), 4 porte ottiche di uplink SFP+ 10 Gbps e 2 porte di stacking (fino a 8 unità per stack) con possibilità di equipaggiare un power supply ridondato. Offre un design ottimizzato per flessibilità e scalabilità con un basso consumo energetico.

L'apparato supporta protocolli di livello 3 di base, incluso VRRP e fornisce switching capacity di 216 Gbps e wire-speed performance su tutte le porte con un power budget PoE pari a 785 Watt al fine di fornire 15,4W di PoE contestuali su tutte le 48 porte utente e in aggiunta la possibilità di load sharing del PoE quando è equipaggiato il secondo alimentatore, per un power budget PoE fino a 1440W. Incluso a corredo il cavo di stack di lunghezza 1 mt.

OmniSwitch 6560 è una soluzione completa per la realizzazione del livello di accesso nelle reti di medie e grandi dimensioni. Utilizza il collaudato Alcatel-Lucent Operating System (AOS) per fornire alta disponibilità, sicurezza, protezione ed è facilmente gestibile.

Supporta innovative soluzioni per la visibilità e la gestione dei dispositivi collegati sulle porte utente (Fingerprinting IoT), in collaborazione con il sistema di gestione OmniVista 2500 (tipo 10 in convenzione), al fine di identificare e classificare il tipo di dispositivo attestato all'apparato, e successivamente attivare delle regole di micro-segmentazione sulla base delle scelte dell'amministratore di rete.

2.4.3. HPE Aruba 2930M 48G PoE+ Switch (JL322AC)

Gli Aruba 2930M, appartenenti alla tipologia 4 in convenzione Consip Lan 7, sono switch Layer 3 Ethernet in grado di supportare diversi servizi: permettono il forwarding IPv6 e offrono alle Amministrazioni quattro porte 10-Gigabit Ethernet (GbE) e power supply da 1050W con possbilità di modulo ridondato interno.

Gli Aruba 2930M condividono le stesse funzionalità Software descritte per gli Aruba 2930F della Tipologia 1 e tipologia 2 ad eccezione della funzionalità di Virtual Chassis. La serie Aruba 2930M offre un accesso da 1-GbE e può essere utilizzata nel perimetro (edge) del network o per collegare i cluster dei server nei data center.

Il Virtual Chassis dei Aruba 2930M viene gestita tramite i moduli di stack Hardware.

La tecnologia brevettata Aruba Stack permette la configurazione di un Virtual Chassis di dimensione massima di dieci apparati, interconnessi tramite un modulo con due porte da 50GbE. Il modulo ed i cavi di connessione sono inclusi in bundle con ogni apparato fornito in convenzione Consip Lan 7.

- Supporto multiservizi

  Gli switch della serie Aruba 2930M supportano le tecnologie PoE+ e LLDP-MED (Media Endpoint Discovery), permettendo agli switch di individuare automaticamente il traffico voce e di accelerare il suo passaggio nel network. Ciò ottimizza il bandwidth per le informazioni time-sensitive e previene efficacemente l'impatto causato da bruschi flussi di dati nello streaming voce. PoE+ permette la trasmissione di dati e di energia nello stesso cavo, facilitando il deployment dei dispositivi collegati al network. Supportando sia la tecnologia PoE+ che LLDP-MED, gli switch della serie Aruba 2930M offrono una soluzione di gestione completa in grado di risolvere molti problemi legati all'"intelligent detection", al sistema di alimentazione e all'impostazione delle priorità, per offrire servizi come la telefonia IP, video-on-demand e lo streaming di materiale multimediale.
- Politiche di controllo sulla sicurezza globale.

Gli switch della serie Aruba 2930M includono il supporto per l'autenticazione 802.1x e l'autenticazione centralizzata degli indirizzi MAC che controlla l'access rights degli utenti al network secondo gli indirizzi MAC e delle porte. Il supporto per Secure Shell Version 2 (SSHv2) garantisce la sicurezza delle informazioni attraverso un potente strumento di autenticazione che previene dagli attacchi al network come lo spoofing degli indirizzi IP e dall'intercettazione di password troppo semplici.

- Eccellente Gestibilità.

  Gli switch della serie Aruba 2930M supportano Simple Network Management Protocol (SNMP) v1/v2c/v3 e possono essere gestiti da Aruba Airwave. Supportano anche command-line interface (CLI), Web network management e Telnet per facilitare la gestione del sistema. Un'altra caratteristica di gestione degli switch della serie Aruba 2930M è di permettere a una rete VLANs di essere classificata nei propri indirizzi MAC, ciò offre all'Amministrazione una gestione intelligente e flessibile delle risorse mobile office in collaborazione con le policy ACL basate su VLANs globali, ottimizzando le risorse hardware e, allo stesso tempo, semplificando la configurazione degli utenti.

- HPE Redundant Power Systems

  Gli switch Aruba 2930M forniscono la possibilità di ridondare internamente l'alimentazione. In convenzione sono presenti, come elementi opzionali, i corrispondenti alimentatori di backup. In particolare, per la tipologia 4 è disponibile il Power Supply X372 54VDC 1050W che consente di raggiungere un power budget PoE+ di 1440W. Per migliorare l'efficienza ed il risparmio energetico, i power supply sono certificati 80 PLUS Gold and Platinum. Il supporto dello standard IEEE 802.3az Energy-efficient Ethernet (EEE) riduce il consumo energetico durante i periodi di inattività.

2.4.4. Huawei S5730-68C-PWR-SI-AC

In fase di sostituzione per End of Sale

2.4.5. ZTE 5950-60PM

La famiglia di switch ZXR10 5950 (1 RU) si compone di apparati installabili a rack 19", gigabit ethernet L3, con funzionalità stackable, ideali per le reti di accesso ed aggregazione. Il prodotto offerto fornisce fino a 52 interfacce (48*GE + 4*10GE), 1 Slot di espansione, 1 GE MNG, 1 RJ45 Console, 1 Mini USB Console, 1 ventola di raffreddamento e doppia alimentazione. Gli switch della serie ZXR10 5950 supportano le seguenti ulteriori funzionalità:

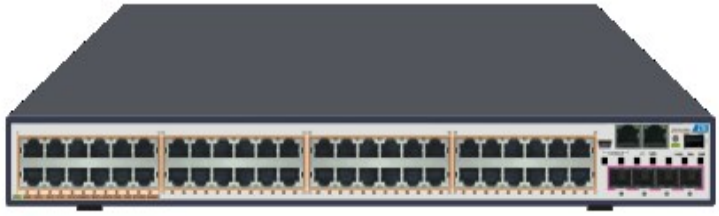
- VSC (Virtual Switch Cluster) 2.0: Fino a 4 apparati sono visti, logicamente, come un unico apparato;
- ZESR – ZTE Ethernet Smart Ring network technology: algoritmo di protezione di un anello in fibra in 10ms;
- Flexible PoE: protezione dalle sovratensioni e possibilità di schedulare l'alimentazione per fasce orarie;

- Zero-touch provisioning: caricamento della prima configurazione tramite Stick USB;
- M-Button: Spie di segnalazione guasti sul fronte dell'apparato.

Il modello proposto è 5950-60PM (Ethernet 10/100/1000 non-PoE/PoE/POE+ con uplink a 10Gb).

L'apparato comprende: 48 porte Ethernet 10/100/1000M RJ45, 4 porte ottiche 10GE SFP+ e 2 moduli di alimentazione AC. La capacità di switching è di 336 Gbps.

L'apparato è gestibile dal sistema di management NetNumen, incluso all'interno della Convenzione (Tipo 10).



2.5. Switch Tipo 5

2.5.1. Juniper EX4300-48MP

Lo switch ethernet EX4300-48MP è un apparato ad alte prestazioni per infrastrutture LAN campus e branch che supportano servizi avanzati. Le infrastrutture moderne, infatti, devono supportare WI-FI 802.11ac Wave II (Wifi 6) e velocità multi-gigabit 1/2.5/5/10GBe con PoE fino a 95W per porta.

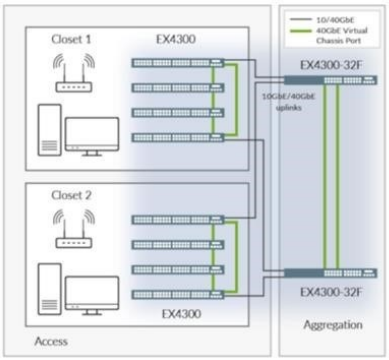
Gli EX4300 sono "cloud-ready" e supportano l'installazione zero-touch (ZTP), che non richiede alcuna configurazione manuale, tramite il servizio di **Wired Assurance**. Gli switch supportano la tecnologia **Virtual Chassis** ed è possibile connettere e gestire fino a 10 switch EX4300 tra loro, come se fossero in singolo apparato logico. Lo switch supporta **MACsec AES256** su tutte le porte di accesso e uplink.

Funzionalità in evidenza

Porte	24 x 1GbE e 24 x 1/2.5/5/10GbE – uplink disponibile a 10/25/40/100GbE
Power	PSU ridondata – PoE/PoE+/PoE++ fino a 95W per porta
Switch capacity	960 Gbps
Fabric	Virtual Chassis fino a 10 switch, EVPN/VxLAN

Virtual Chassis

La tecnologia Virtual Chassis permette di collegare fino a 10 EX4300 e di gestirli come un solo apparato, riducendo i costi operativi e semplificando la gestione. La configurazione in Virtual Chassis garantisce alta affidabilità e semplifica il disegno della rete.



MACsec AES256

Gli switch EX4300 supportano IEEE 802.1ae MACsec AES256 e garantiscono la confidenzialità, integrità e autenticità della comunicazione dei dati a livello link-layer.

PoE++

Lo switch EX4300 Multi gigabit supporta lo standard 802.3bt e fornisce fino a 95watts per porta per dispostivi ad alto assorbimento come terminali Virtual Desktop Infrastructure (VDI), telefono IP, APs.

Campus Fabric

Lo switch supporta fabric IP con overlay EVPN-VxLAN. La fabric può estendere la connettività tra più siti e realizzare l'estensione a livello 2 della rete (L2 stretch).

2.5.2. ALE OS6860N-P48MZC

In fase di sostituzione per End of Sale

2.5.3. HPE Aruba – 2930M 40 G 8SR (R0M67AC)

Gli Aruba 2930M, appartenenti alla tipologia 5 in convenzione Consip Lan 7, sono switch Layer 3 Ethernet in grado di supportare diversi servizi: permettono il forwarding IPv6 e offrono alle Amministrazioni quattro porte 10-Gigabit Ethernet (GbE), 8 porte MultiGigabit Ethernet e power supply da 1050W con possbilità di modulo ridondato interno. Gli Aruba 2930M condividono le stesse funzionalità Software descritte per gli Aruba 2930F della Tipologia 1 e tipologia 2 ad eccezione della funzionalità di Virtual Chassis. La serie Aruba 2930M offre un accesso da 1-GbE e può essere utilizzata nel perimetro (edge) del network o per collegare i cluster dei server nei data center.

Il Virtual Chassis dei Aruba 2930M viene gestita tramite i moduli di stack Hardware.

La tecnologia brevettata Aruba Stack permette la configurazione di un Virtual Chassis di dimensione massima di dieci apparati, interconnessi tramite un modulo con due porte da 50GbE. Il modulo ed i cavi di connessione sono inclusi in bundle con ogni apparato fornito in convenzione Consip Lan 7.

- Supporto multiservizi

  Gli switch della serie Aruba 2930M supportano le tecnologie PoE+ e LLDP-MED (Media Endpoint Discovery), permettendo agli switch di individuare automaticamente il traffico voce e di accelerare il suo passaggio nel network. Ciò ottimizza il bandwidth per le informazioni time-sensitive e previene efficacemente l'impatto causato da bruschi flussi di dati nello streaming voce. PoE+ permette la trasmissione di dati e di energia nello stesso cavo, facilitando il deployment dei dispositivi collegati al network. Supportando sia la tecnologia PoE+ che LLDP-MED, gli switch della serie Aruba 2930M offrono una soluzione di gestione completa in grado di risolvere molti problemi legati all'"intelligent detection", al sistema di alimentazione e all'impostazione delle priorità, per offrire servizi come la telefonia IP, video-on-demand e lo streaming di materiale multimediale.

- Politiche di controllo sulla sicurezza globale.

  Gli switch della serie Aruba 2930M includono il supporto per l'autenticazione 802.1x e l'autenticazione centralizzata degli indirizzi MAC che controlla l'access rights degli utenti al network secondo gli indirizzi MAC e delle porte. Il supporto per Secure Shell Version 2 (SSHv2) garantisce la sicurezza delle informazioni attraverso un potente strumento di autenticazione che previene dagli attacchi al network come lo spoofing degli indirizzi IP e dall'intercettazione di password troppo semplici.

- Eccellente Gestibilità.

  Gli switch della serie Aruba 2930M supportano Simple Network Management Protocol (SNMP) v1/v2c/v3 e possono essere gestiti da Aruba Airwave. Supportano anche command-line interface (CLI), Web network management e Telnet per facilitare la gestione del sistema. Un'altra caratteristica di gestione degli switch della serie Aruba 2930M è di permettere a una rete VLANs di essere classificata nei propri indirizzi MAC, ciò offre all'Amministrazione una gestione intelligente e flessibile delle risorse mobile office in collaborazione con le policy ACL basate su VLANs globali, ottimizzando le risorse hardware e, allo stesso tempo, semplificando la configurazione degli utenti.

- HPE Redundant Power Systems

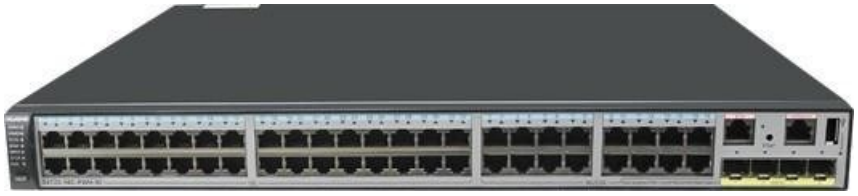
Gli switch Aruba 2930M forniscono la possibilità di ridondare internamente l'alimentazione. In convenzione sono presenti, come elementi opzionali, i corrispondenti alimentatori di backup. In particolare, per la tipologia 5 è disponibile il Power Supply X372 54VDC 1050W che consente di raggiungere un power budget PoE+ di 1440W. Per migliorare l'efficienza ed il risparmio energetico, i power supply sono certificati 80 PLUS Gold and Platinum. Il supporto dello standard IEEE 802.3az Energy-efficient Ethernet (EEE) riduce il consumo energetico durante i periodi di inattività.

2.5.4. Huawei S6720-56C-PWH-SI-AC

Il modello Ethernet Switch S6720-56C-PWH-SI-AC fa parte della series S6720SI. È uno switch Full Layer 3 con supporto di IP routing avanzato (statico, RIP e OSPF, IS-IS, BGP4+), ECMP, di protocolli di affidabilità (VRRP) e migliori specifiche tecniche per essere dispiegato sia come switch di Accesso per le interfacce Multigigabit Ethernet (2.5/5G) che di Aggregazione. Installabile a rack 19", equipaggia 32 porte 10/100/1000 PoE++ e 16 porte 100M/1G/2.5G/5G/10G Ethernet su rame e 4 porte 10GE (autosensing @1GE) ottico su SFP+. In dotazione è fornito un cavo di stack da 1 metro e un modulo da 4 porte 10GE sul retro. In termini di alimentazione, è dotato e fornito con un un alimentatore estraibile in AC che può essere ridondato nell'opportuno slot sul retro dell'apparato.

Ha una matrice di switching non blocking con inoltro del traffico in modalità wirespeed e capacità di processamento pacchetti pari a 240 Mpps (milioni di pacchetti per secondo), supporta funzionalità di multicast di livello 2 e livello 3 (IGMP, MLD, PIM) e meccanismi loop prevention di livello 2 sia per reti ad anello che ad albero.

È gestibile (configurazione, monitoraggio e allaramistica) dal sistema di management eSight (Tipo 10) incluso all'interno della Convenzione.



2.5.5. ZTE 5950-54PM-H-C

In fase di sostituzione per End of Sale

2.6. Switch Tipo 6

2.6.1. Juniper EX4300-48P

Lo switch ethernet EX4300-48P è un apparato ad alte prestazioni per infrastrutture LAN campus e branch che supportano servizi avanzati. Supporta IEEE 802.3af Power over Ethernet e 802.3at PoE+ fino a 30W per porta.

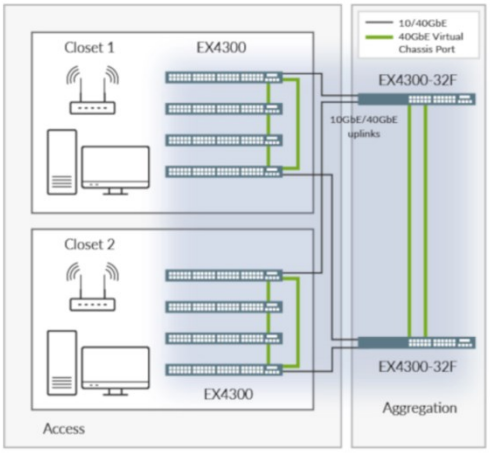
Gli EX4300 sono "cloud-ready" e supportano l'installazione zero-touch (ZTP), che non richiede alcuna configurazione manuale, tramite il servizio di **Wired Assurance**. Gli switch supportano la tecnologia **Virtual Chassis** ed è possibile connettere e gestire fino a 10 switch EX4300 tra loro, anche in mixed stacking con apparati EX4600, come se fossero in singolo apparato logico.

Funzionalità in evidenza

Porte	48 x 1GbE e 4 SFP+ 10Gbe e 4 QSFP+ 40GbE
Power	PSU ridondata – PoE/PoE+ fino a 30W per porta
Switch capacity	496 Gbps
Fabric	Virtual Chassis fino a 10 switch anche mixed con EX4600

Virtual Chassis

La tecnologia Virtual Chassis permette di collegare fino a 10 EX4300 e/o EX4600 e di gestirli come un solo apparato, riducendo i costi operativi e semplificando la gestione. La configurazione in Virtual Chassis garantisce alta affidabilità e semplifica il disegno della rete.



MACsec

Gli switch EX4300 supportano IEEE 802.1ae MACsec e garantiscono la confidenzialità, integrità e autenticità della comunicazione dei dati a livello link-layer.

QoS con 12 code di priorità

Lo switch ha 12 code, 8 unicast e 4 multicast, per porta, che assicurano la gestione della priorità del traffico voce, video e di molteplici classi di traffico dati e permettendo, ad esempio, la gestione della QoS per reti dedicata al building automation o ai sistemi di video sorveglianza.

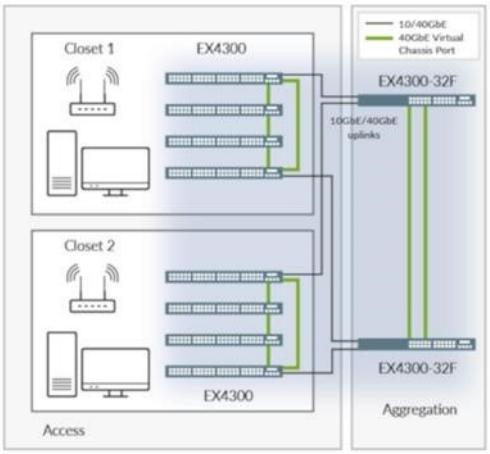


Figure 2: Using Virtual Chassis technology, up to 10 EX4300 switches can be interconnected to create a single logical device spanning an entire building.

2.6.2. ALE OS6860-P48C

In fase di sostituzione per End of Sale

2.6.3. HPE Aruba 3810M 48G PoE+ 4SFP+ (JL429AC)

Gli switch HPE Aruba 3810M, appartenenti alla tipologia 6 in convenzione Consip Lan 7, offrono ottime prestazioni e resilienza per reti di grandi aziende, piccole e medie imprese e filiali. Con porte multi-gigabit HPE Smart Rate per dispositivi 802.11 AC ad alta velocità, questo avanzato switch Layer 3 offre una migliore esperienza dell'applicazione con bassa latenza, la virtualizzazione con tecnologia di stacking resiliente e velocità a 40 GbE, per il massimo della capacità possibile. Gli switch Aruba 3810 sono facili da implementare e da gestire, con sicurezza e strumenti di gestione di rete avanzati quali ClearPass Policy Manager, Aruba AirWave e Aruba Central su Cloud.

La serie di switch 3810 Aruba è una soluzione leader nel settore per l'accesso mobile a reti di tipo campus per le aziende, le piccole e medie aziende e le reti di sedi distaccate. Con porte SFP multi-gigabit HPE Smart Rate per i dispositivi ad alta velocità 802.11ac, il modello Aruba 3810 preparerà la rete per il futuro.

Le porte HPE Smart supportano velocità Ethernet multi-gigabit (Ethernet a 1, 2.5, 5 e 10 gigabit) sul cablaggio esistente per aggiornamenti della rete che siano efficienti e convenienti, senza la necessità di rimuovere e sostituire il cablaggio.

Ottimizzato per la postazione di lavoro digitale grazie agli strumenti di gestione e sicurezza unificati quali Aruba ClearPass Policy Manager, Aruba Airwave e Aruba Central. Offre una configurazione ottimale automatica quando collegato agli access point Aruba per priorità PoE, configurazione VLAN e per il contenimento di punti d'accesso non autorizzati.

Implementazione delle dimensioni necessarie e capacità back-haul con uplink modulari da 10 GbE.

Provisioning PoE+ completo su 48 porte. Alimentatori doppi, ridondanti, hot-swap e un'innovativa tecnologia di backplane che offre flessibilità e scalabilità in un conveniente fattore di forma 1U.

Set di funzionalità avanzate Layer 2 e 3 con OSPF, IPv6, IPv4 BGP, una robusta QoS e routing basato su policy sono inclusi senza licenze software. L'interfaccia REST API integrata, programmabile e facile da usare, fornisce l'automazione di configurazione per reti campus mobile-first.

- Resilienza ed elevata disponibilità su cui poter contare

  La serie di switch 3810 Aruba è progettata con un ASIC ProVision progettato per realizzare una rete campus mobile con bassissima latenza, un buffer di pacchetti maggiore e un consumo energetico adattivo. La tecnologia stacking backplane offre stacking ad alte prestazioni con un massimo di 336 Gb/s di throughput di stacking e una maggiore resilienza. È possibile impilare fino a dieci switch 3810 in una topologia ad anello o fino a cinque in una topologia mesh.

Due alimentatori hot-swap offrono l'alimentazione e consentono lo scambio dei moduli in tempo reale per ridurre l'impatto sulla disponibilità della rete. Aumento delle prestazioni grazie alla possibilità di selezionare il numero di code e buffer di memoria associato che soddisfa nel modo migliore i requisiti delle applicazioni di rete con priorità.

La possibilità di selezionare il numero di code consente l'incremento delle prestazioni con la selezione del numero di code e buffer di memoria associato che soddisfa al meglio le esigenze delle applicazioni di rete.

Switching e Routing senza interruzioni per una migliore fruibilità e una maggiore L3 disponibilità delle applicazioni. Supporta il protocollo di ridondanza del router virtuale (VRRP) che consente a gruppi di due router di eseguire reciprocamente il backup in modo dinamico per creare ambienti di router ad alta disponibilità nelle reti IPv4 e IPv6.

- Sicurezza affidabile con una straordinaria QoS

  La serie di switch Aruba 3810 include un set completo di funzionalità di protezione e QoS per la creazione di una rete solida, in grado di soddisfare le esigenze aziendali in termini di policy e conformità. Controlli del traffico flessibili, come routing basato su policy, QoS e ACL per la gestione delle priorità delle applicazioni end-to-end, al fine di assicurare una migliore esperienza utente.

  Sicurezza avanzata e applicazioni basate su policy, con modalità di autenticazione simultanee 802.1X, MAC e Web. Previene il traffico indesiderato con funzionalità di protezione avanzata DDOS (Distributed Denial of Service) quali DHCP Snooping, IP Source Guard e ARP Protection. Efficaci controlli di sicurezza con più livelli di accesso, ad esempio la gestione basata su ruoli, la complessità della password configurabile, RADIUS/TACACS+ e SSH per una migliore protezione e controllo dell'accesso alla gestione delle modifiche. Nodi con tunnel, per trasportare il traffico di rete a livello di porta al controller Aruba, con autenticazione e policy di rete applicate e rafforzate sul controller. Lo standard del settore MACsec fornisce protezione a livello di collegamento switch-to-switch.

- Semplificazione grazie alla gestione unificata

  La serie di switch Aruba 3810 supporta ClearPass Policy Manager per fornire una policy unificata e costante tra utenti cablati e wireless. Implementazione e gestione semplificate dell'accesso guest, accettazione degli utenti, accesso alla rete, sicurezza, QoS e altre policy di rete. Supporta il software AirWave e Aruba Central basato su cloud per fornire una piattaforma comune per la gestione zero-touch del provisioning e il monitoraggio per dispositivi di rete cablati e wireless. Supporta Central basato su cloud e AirWave on-premise con lo stesso hardware, garantendo che il cambiamento della piattaforma di gestione non renda necessaria una sostituzione integrale dell'infrastruttura di switch. RMON, XRMON e sFlow forniscono funzionalità avanzate di monitoraggio e reporting per statistiche, cronologia, avvisi

ed eventi. La porta di gestione Ethernet fuori banda mantiene il traffico di gestione separato dal traffico dei dati di rete.

2.6.4. Huawei S5730-60C-PWH-HI

In fase di sostituzione per End of Sale

2.6.5. ZTE 5950-56PM-H

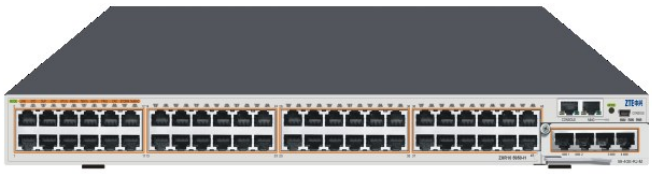
La famiglia di switch ZXR10 5950-H (1 RU) si compone di apparati ad alta densità di porte, installabili a rack 19", gigabit ethernet L3, con funzionalità stackable, ideali per le reti di accesso ed aggregazione. Il prodotto offerto fornisce fino a 56 interfacce (48*GE non-PoE/PoE/POE+/UPOE + 8*10GE), 1 GE MNG, 1RJ45 Console, 1 Mini USB Console, 2 ventole di raffreddamento e doppia alimentazione. Gli switch della serie ZXR10 5950-H supportano le seguenti ulteriori funzionalità:

- VSC (Virtual Switch Cluster) 2.0: Fino a 4 apparati sono visti, logicamente, come un unico apparato;
- ZESR – ZTE Ethernet Smart Ring network technology: algoritmo di protezione di un anello in fibra in 10ms;
- Zero-touch provisioning: caricamento della prima configurazione tramite Stick USB;
- M-Button: Spie di segnalazione guasti sul fronte dell'apparato.

Il modello proposto è 5950-56PM-H (Ethernet 10/100/1000 con uplink a 10Gb).

L'apparato comprende: 48 porte Ethernet 10/100/1000M RJ45, 8 porte ottiche 10GE SFP+ e 2 moduli di alimentazione AC. La capacità di switching è di 336 Gbps.

L'apparato è gestibile dal sistema di management NetNumen, incluso all'interno della Convenzione (Tipo 10).



2.7. Switch Tipo 7

2.7.1. Juniper EX4300-32F

Lo switch ethernet EX4300-32F è un apparato ad alte prestazioni per infrastrutture LAN campus e branch che supportano servizi avanzati. Il sistema operativo dello switch, Junos OS, supporta funzionalità di switching L2 e L3, routing e servizi di security, e grazie al design modulare, garantisce la massima affidabilità e disponibilità della rete.

Anche le caratteristiche hardware garantiscono l'alta affidabilità, grazie ad alimentatori e ventole ridondate e hot-swap.

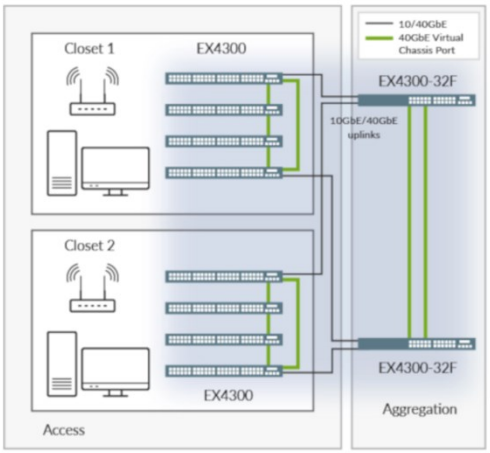
Gli EX4300 sono "cloud-ready" e supportano l'installazione zero-touch (ZTP), che non richiede alcuna configurazione manuale, tramite il servizio di **Wired Assurance**. Gli switch supportano la tecnologia **Virtual Chassis** ed è possibile connettere e gestire fino a 10 switch EX4300 tra loro, anche in mixed stacking con apparati EX4600, come se fossero in singolo apparato logico.

Funzionalità in evidenza

Porte	32 x 1GbE SFP - 4 SFP+ 10Gbe e 2 QSFP+ 40GbE
Power	PSU ridondata e hot-swap
Switch capacity	464 Gbps
Fabric	Virtual Chassis fino a 10 switch anche mixed con EX4600

Virtual Chassis

La tecnologia Virtual Chassis permette di collegare fino a 10 EX4300 e/o EX4600 e di gestirli come un solo apparato, riducendo i costi operativi e semplificando la gestione. La configurazione in Virtual Chassis garantisce alta affidabilità e semplifica il disegno della rete.



MACsec

Gli switch EX4300 supportano IEEE 802.1ae MACsec e garantiscono la confidenzialità, integrità e autenticità della comunicazione dei dati a livello link-layer.

QoS con 12 code di priorità

Lo switch ha 12 code, 8 unicast e 4 multicast, per porta, che assicurano la gestione della priorità del traffico voce, video e di molteplici classi di traffico dati e permettendo, ad esempio, la gestione della QoS per reti dedicata alla building automation o ai sistemi di video sorveglianza.

2.7.2. ALE OS6860E-U28C

Alcatel-Lucent Enterprise OmniSwitch® 6860E è una famiglia di Switch Ethernet Layer 3 Stackable avanzata con porte Gigabit che offre Alte Performance, scalabilità, resilienza e sicurezza.

Il modello in oggetto è uno Switch Layer 3 a forma compatta per inserimento in armadio a 19 pollici che fornisce 28 porte ottiche SFP 1000BaseX unpopoled e 4 porte ottiche SFP+ 1G oppure 10GBaseX per il collegamento in uplink. L'apparato dispone di 2 porte QSFP+ 20Gbps per lo stacking (fino a 8 unità per stack).

L'apparato supporta protocolli di livello 3 avanzati, unicast e multicast e fornisce switching capacity di 224 Gbps e wire-speed performance su tutte le porte Incluso a corredo il cavo di stack di lunghezza 1 mt. Questo modello include co-processore per il fingerprinting applicativo, e l'enforcement di regole di QoS o ACL di livello 7.

È un apparato con un elevato grado di sicurezza integrata grazie a funzionalità di macro e micro-segmentazione, indispensabili per segregare dispositivi e applicazioni e mantenere un elevato controllo dell'accesso della rete.

In aggiunta la disponibilità di MACsec permette di incrementare la confidenzialità e l'integrità dei dati a livello di link-layer, per indirizzare esigenze di sicurezza sui collegamenti di uplink.

Grazie alla sua versatilità e alla completa dotazione di funzionalità, è la giusta scelta per l'implementazione del livello di aggregazione delle reti aziendali di medie dimensioni o come apparato di core di reti piccole dove esiste l'esigenza di raccogliere la connettività di uplink a 1Gigabit Ethernet proveniente dal livello di accesso, su un apparato solido e performante.

2.7.3. HPE ARUBA 5510 24G SFP 4SFP+ HI (JH149AC)

Gli switch HPE 5510-HI, appartenenti alla tipologia 7 in convenzione Consip Lan 7, offrono una sicurezza eccezionale, alta affidabilità e supporto multi-service per lo switching di aggregation-layer per grandi aziende e campus network, o per il core-layer delle aziende di piccole e medie dimensioni. La serie comprende switch Gigabit Ethernet (GbE) Layer 2/3/4 che possono adattarsi alle applicazioni più richieste, offrendo una connettività resiliente e sicura, oltre che tecnologie per la prioritizzazione del traffico per ottimizzare le applicazioni nel network convergente.

Progettati per raggiungere il massimo della flessibilità, questi switch sono disponibili in convenzione con 24 porte SFP 1-GbE, di cui 8 dual ports (SFP o RJ45), 4 porte SFP+. Per raggiungere un maggior livello di flessibilità, entrambi gli switch presentano uno slot di espansione in cui poter inserire moduli con connettività 10GbE o 40GbE. Inoltre, è importante sottolineare che entrambi i modelli proposti presentano la possibilità di ridondare l'alimentatore internamente allo switch.

La tecnologia brevettata HPE Intelligent Resilient Framework (IRF) permette l'interconnessione di massimo nove switch. Ciò facilità la creazione di un network completamente ridondato: le porte aggregate sono distribuite su più unità e gli switch utilizzano un'unica interfaccia di gestione.

Il modello della serie 5510-HI presente in convenzione viene consegnato in un pratico enclosure "stackable" 1U.

- Quality of Service (QoS)

  Il sistema di classificazione avanzata QoS classifica il traffico utilizzando diversi parametri basati sulle informazioni dei Layer 2, 3 e 4; applica le policy QoS -come le impostazioni sui livelli di priorità e il limite del traffico selezionato- secondo il tipo di porta o di VLAN. La serie di switch applica le policy sulle limitazioni di traffico supportando Committed Access Rate (CAR) e la velocità di linea. Questa serie di switch crea diverse classi di traffico in base alla lista di controllo d'accesso (access control lists - ACL), alle preferenze IEEE 802.1p, IP, DSCP o al tipo si servizio (Type of Service - ToS); supporta filtraggio, re-indirizzamento, mirroring e funzioni di nota; supporta le seguenti azioni di congestione: strict priority (SP) queuing, weighted round robin (WRR), weighted fair queuing (WFQ), weighted random early discard (WRED), weighted deficit round robin (WDRR) e SP+WDRR. Un'altra importante caratteristica consente di limitare il broadcast, multicast e il traffico unicast sconosciuto per abbattere notevolmente il traffico network non desiderato.

- Gestione

  La gestione avviene attraverso semplici caratteristiche -come la configurazione e la gestione in remoto- disponibili tramite un browser Web sicuro o un'interfaccia command-line (CLI). Un Web GUI sicuro fornisce un'interfaccia grafica semplice da gestire per la configurazione del modulo HTTPS. I livelli preferiti del manager e degli operatori permettono accesso di sola lettura (operatore) e sola scrittura (manager) su interfacce di gestione CLI e Web. Inoltre, è possibile utilizzare RADIUS per collegare una lista di comandi CLI del cliente ad un login individuale da parte dell'amministratore. Altre caratteristiche di gestione includono SNMPv1, v2c e v3 per facilitare individuazione, monitoraggio centralizzati e gestione sicura dei dispositivi network.

- Connettività

  La serie HPE 5510 HI offre un livello superiore di connettività. Le caratteristiche includono Auto-MDIX che regola automaticamente i cavi su porte 10/100 e 10/100/1000. Quattro porte SFP+ fisse da 10GbE. Il bundle comprende un modulo con 2 porte 40 GbE QSFP+ ed un cavo DAC della lunghezza di 1m.

- Prestazioni

  Gli switch HPE 5510 HI offrono una lista di controllo per l'accesso (ACL) caratterizzata da implementazioni ACL (basate su TCAM), che aiuta a garantire alti livelli di sicurezza e semplicità di amministrazione senza impattare le prestazioni del network. Fino a 336 Gpps di fabric switch "non-blocking" per fornire capacità switch a velocità di cavo con fino a 250 Mpps di throughput.

- Resilienza e Alta Disponibilità

  Intelligent Resilient Framework (IRF) crea fabric switch resilienti virtuali in cui due o più switch realizzano funzioni di router come un singolo switch Layer 2 e 3. Grazie a questa caratteristica, gli switch non devono trovarsi nella stessa locazione e possono essere parte di un sistema di disaster-recovery. I server e gli switch possono essere uniti attraverso LACP standard per il bilanciamento automatico dei carichi e alta disponibilità, per sempificare le operazioni network ed eliminare la complessità di Spanning Tree Protocol, Equal-Cost Multipath (ECMP) o VRRP.

- Routing Layer 3

  I servizi di routing Layer 3 sono forniti attraverso i protocolli di routing IPv4 che supportano il routing statico come RIP, OSPF, ISIS e BGP. La connettività è sempificata attraverso Virtual Private LAN Service (VPLS) che stabilisce il VPN Layer 2 "point-to-multipoint" sul provider del network.

- Sicurezza

  La sicurezza è un elemento fondamentale negli ambienti IT odierni e la serie di switch 5510 HI supporta una vasta gamma di strumenti di protezione. Il controllo dell'identità durante l'accesso è garantito da per-user access control lists (ACLs), assegnazione automatica della VLAN. L'accesso è controllato

mediante ACL che forniscono meccanismi di filtraggio di traffico IP dal Layer 2 al Layer 4; supporta porte global ACL, VLAN ACL e IPv6 ACL. IEEE 802.1X, un metodo per l'autenticazione degli utenti, un IEEE 802.1X supplicant sul client con server RADIUS.

2.7.4. Huawei S5730-44C-HI-24S

In fase di sostituzione per End of Sale

2.7.5. ZTE 5960-32DL

La famiglia di switch ZXR10 5960 (1RU) si compone di apparati switch, installabili a rack 19", next-generation carrier-grade per data center normalmente definiti TOR (Top of Rack) con capacità di switching ultra-larga e low latency. La famiglia ZXR10 5960 offre reliability carrier-class e scalabilità superiore. Gli apparati della famiglia ZXR10 5960 offrono complete funzionalità tipiche da data center: VSC (Virtual Switch Cluster), TRILL (Transparent Interconnection of Lots of Links), SDN (Software Defined Network), Front-to-back airflow. Il prodotto offerto fornisce fino a 32 interfacce (24*10GE SFP+ + 2*40GE – ogni porta a 40GE può essere splittata in 4 porte 10GE), 1 RJ45 Console, 1 Mini USB Console, 1 GE Combo MNG, 1 USB, 2 ventole di raffreddamento e doppia alimentazione. Gli switch della serie ZXR10 5960 supportano le seguenti ulteriori funzionalità:

- VSC (Virtual Switch Cluster) 2.0: Fino a 4 apparati sono visti, logicamente, come un unico apparato;
- ZESR – ZTE Ethernet Smart Ring network technology: algoritmo di protezione di un anello in fibra in 10ms;
- Service Quality Analyzer: lo switch è in grado di inviare pacchetti ad un server per misurare la qualità della linea;
- Zero-touch provisioning: caricamento della prima configurazione tramite Stick USB;
- M-Button: Spie di segnalazione guasti sul fronte dell'apparato.

Il modello proposto è: 5960-32DL (layer 3 - 24 Porte SFP+ con uplink a 40Gb). L'apparato comprende: 24* 10GE SFP+ ports, 2* 40GE QSFP+ ports, 2 moduli di alimentazione AC. La capacità di switching è di 640 Gbps. L'apparato è gestibile dal sistema di management NetNumen, incluso all'interno della Convenzione (Tipo 10).

2.8. Switch Tipo 8

2.8.1. Juniper EX4600-40F-AFO

Lo switch EX4600 è un apparato compatto ad alte prestazioni ed elevate scalabilità (offre fino a 72 porte 10Gbe in 1RU) ideale come apparato di distribuzione e core in ambito campus e come top-of-rack in ambito data center. Il sistema operativo dello switch, Junos OS, supporta funzionalità L2 e L3, routing e servizi di security, e grazie al design modulare, garantisce la massima affidabilità e disponibilità della rete. Anche le caratteristiche hardware garantiscono l'alta affidabilità, grazie ad alimentatori e ventole ridondate e hot-swap.

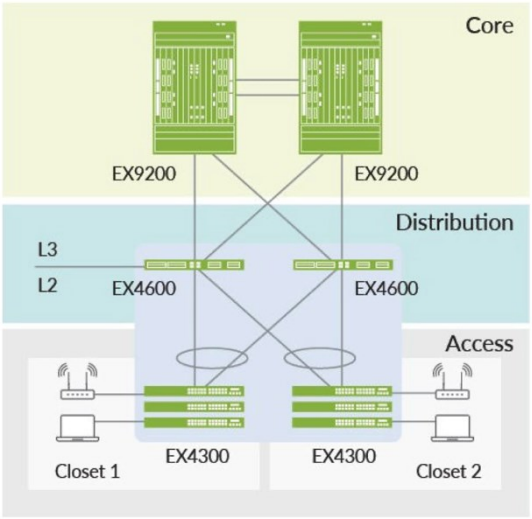
Gli EX4600 sono "cloud-ready" e supportano l'installazione zero-touch (ZTP), che non richiede alcuna configurazione manuale, tramite il servizio di **Wired Assurance**. Gli switch supportano la tecnologia **Virtual Chassis** ed è possibile connettere e gestire fino a 10 switch EX4600 tra loro, anche in mixed stacking con apparati EX4300, come se fossero in singolo apparato logico.

Funzionalità in evidenza

Porte	40 porte 1/10G di tipo SFP/SFP+ e 4 porte 40G QSFP+.
Power	PSU ridondata e hot-swap, consumo < 5W per 10Gbe
Switch capacity	1.44 Tbps
Fabric	Virtual Chassis fino a 10 switch – MC-LAG

Virtual Chassis

La tecnologia Virtual Chassis permette di collegare fino a 10 EX4600 e/o EX4300 e di gestirli come un solo apparato, riducendo i costi operativi e semplificando la gestione. La configurazione in Virtual Chassis garantisce alta affidabilità e semplifica il disegno della rete.



MACsec

Gli switch EX4600 supportano IEEE 802.1ae MACsec e garantiscono la confidenzialità, integrità e autenticità della comunicazione dei dati a livello link-layer.

Campus Fabric

Lo switch supporta fabric IP con overlay EVPN-VxLAN. La fabric può estendere la connettività tra più siti e realizzare l'estensione a livello 2 della rete (L2 stretch).

MPLS

EX4600, unico switch compatto nel mercato, supporta un ampio ventaglio di funzionalità MPLS, tra cui L2VPN e L3VPN, e Metro Ethernet.

2.8.2. ALE OS6900-X72-FC

Alcatel-Lucent Enterprise OmniSwitch® 6900 è una famiglia di Switch Ethernet compatti, Layer 3, Stackable con porte ad alta densità a 10G/25G/40G/100G, ideali per soluzioni di rete LAN e datacenter.

Sono apparati ad alte prestazioni con latenza estremamente bassa e supportano protocolli avanzati di routing.

Il modello in oggetto è uno Switch Layer 3 a forma compatta per inserimento in armadio a 19 pollici che fornisce 48 porte ottiche SFP+ unpopoled 1G oppure 10GBaseX e 6 porte ottiche QSFP+ 40GBaseX per il collegamento in uplink o per la realizzazione del virtual chassis (POD). Il dispositivo fornisce switching capacity di 1440 Gbps e wire-speed performance su tutte le porte. In aggiunta il modello supporta tecnologie di virtualizzazione di rete come SBP-M (IEEE 802.1aq). Fornito a corredo il cavo di stack di lunghezza 1 mt. Questo modello prevede la possibilità di alimentazione ridondata con codice aggiuntivo OS6900-BP-F (previsto in convenzione).

La virtualzzazione di nodo permette di realizzare POD con 6 apparati, interconnessi tra di loro con una topologia full mesh, per consentire visibilità diretta tra ogni elemento del cluster e fornire alta affidabilità, scalabilità, bassa latenza e alta banda passante al traffico trasportato nel POD

Questi switch per la loro robustezza, flessibilità e performance sono ideali per i livelli di core e distribution delle reti mission-critical oppure per la realizzazione di fabric nelle server farm.

2.8.3. HPE ARUBA FF 5940 2-slot (JH397AC)

In fase di sostituzione per End of Sale

2.8.4. Huawei S6720-54C-EI-48S-AC

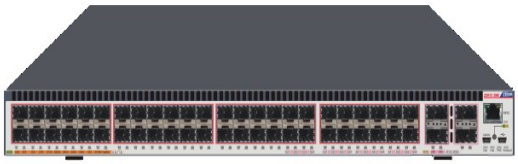
In fase di sostituzione per End of Sale

2.8.5. ZTE 5960-64DL-H

La famiglia di switch ZXR10 5960-H (1RU) si compone di apparati switch, installabili a rack 19", ad alta densità di porte, next-generation carrier-grade per data center normalmente definiti TOR (Top of Rack) con capacità di switching ultra-larga e low latency. La famiglia ZXR10 5960 offre reliability carrier-class e scalabilità superiore. Gli apparati della famiglia ZXR10 5960 offrono complete funzionalità tipiche da data center: VSC (Virtual Switch Cluster), DCB (Data Center Bridging), TRILL (Transparent Interconnection of Lots of Links), VxLAN, FCoE (Fiber Channel over Ethernet, SDN (Software Defined Network), Front-to-back airflow. Il prodotto offerto fornisce fino a 64 interfacce (48*10GE SFP+ + 4*40GE – ogni porta a 40GE può essere splittata in 4 porte 10GE), 1 GE optical Management Port, 1 RJ45 console port, 1 Mini USB console port, 2 ventole di raffreddamento e doppia alimentazione. Gli switch della serie ZXR10 5960-H supportano le seguenti ulteriori funzionalità:

- VSC (Virtual Switch Cluster) 2.0: Fino a 4 apparati sono visti, logicamente, come un unico apparato;
- ZESR – ZTE Ethernet Smart Ring network technology: algoritmo di protezione di un anello in fibra in 10ms;
- Zero-touch provisioning: caricamento della prima configurazione tramite Stick USB.

Il modello proposto è: 5960-64DL-H (layer 3 - 48 Porte SFP+ con uplink a 40Gb). L'apparato comprende: 48* 10GE SFP+ ports, 4* 40GE QSFP+ ports, 2 moduli di alimentazione AC. La capacità di switching è di 6.4 Tbps. L'apparato è gestibile dal sistema di management NetNumen, incluso all'interno della Convenzione (Tipo 10).



2.9. Switch Tipo 9

2.9.1. Juniper EX9204-RED3B-AC

Lo switch EX9204 è un apparato flessibile, scalabile, programmabile, grazie all'asic Junos One, progettato per le infrastrutture di rete a supporto delle applicazioni critiche. Nelle reti enterprise campus, EX9204 è ideale per supportare applicazioni IT moderne quali gli ambienti di collaboration e multimediali.

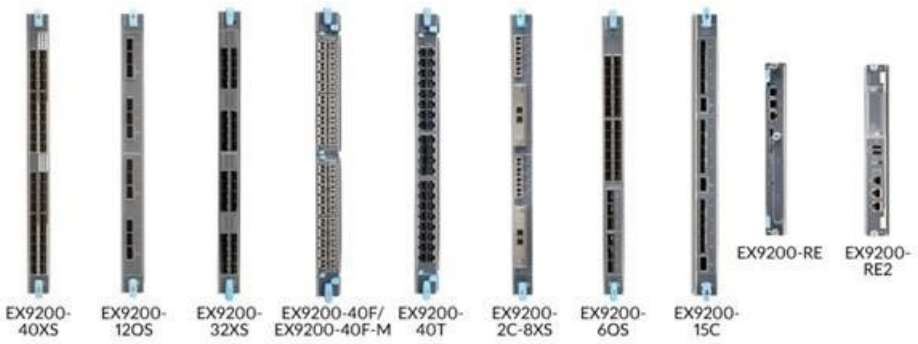
Lo switch di Core EX9204 mette a disposizione delle aziende le più moderne architetture di rete, e grazie alle funzionalità **Ethernet VPN (EVPN) – Virtual Extensible LAN (VXLAN)**, permette di estendere a livello 2 e a livello 3 le reti aziendali. EVPN-VXLAN si basa su standard aperti, e permette di realizzare infrastrutture di rete, geograficamente distribuite, ma coerenti dal punto di vista delle policy di rete, di servizi e di sicurezza.

Funzionalità in evidenza

Form Factor	4 slot Chassis Modulare, 5RU
Porte	Fino a 120 1GbE, 144 10GbE, 120 25GbE, 30 40GbE, 30 100GbE
Power	4 x PSU ridondati e hot-swap; FAN ridondate e hot swap
Switch capacity	fino a 3Tbps per chassis; ridondate
Fabric	EVPN-VXLAN, ESI-LAG, MC-LAG
MAC Address	1 milion
IP Address	1 milion IPv4 e IPv6

EX9200 line cards

Tutte le line card sono basate sul chipset Junos ONE di Juniper, che implementa una vasta serie di funzionalità Layer 2 e Layer 3 incluse: 802.1Q VLAN, link aggregation, Virtual Router Redundancy Protocol (VRRP), L2 to L3 mapping, e port monitoring. In aggiunta le line card supportano filtering, sampling, load balancing, rate limiting, class of service (CoS), e altre funzionalità necessarie per le reti ad alte prestazioni.



MACsec

Gli switch supportano IEEE 802.1ae MACsec e garantiscono la confidenzialità, integrità e autenticità della comunicazione dei dati a livello link-layer, minimizzando i rischi di denial of service (DoS) e altre minacce di sicurezza.

Campus Fabric

Gli switch sono collegati e configurati come una Fabric IP, utilizzando EVPN-VXLAN come overlay. In questo modo la fabric può collegare diversi edifici, ad esempio in una rete campus, e tramite VXLAN è possibile estendere la connettività di livello 2 su tutta l'infrastruttura.

2.9.2. ALE OS9907-RCB-A

La piattaforma chassis modulare Alcatel-Lucent Enterprise OmniSwitch® 9900 è uno switch Ethernet con elevata capacità e alte prestazioni, ideale come Core nelle reti Campus LAN o nel Data Center

OmniSwitch 9900 utilizza il sistema operativo Alcatel-Lucent (AOS), progettato allo stato dell'arte per offrire continuità del servizio sulle reti mission-critical con inoltro del traffico non-stop a livello 2 e livello3.

La piattaforma offre scalabilità lineare della capacità di commutazione mediante la tecnologia di chassis virtuale che fornisce fino a 10 Terabit di capacità di commutazione aggregata. In particolare, il suo design modulare offre protezione degli investimenti con futuri aggiornamenti in linea che offrono alta densità di Interfacce 1G/10G/40G e il supporto del 100G Ethernet a garanzia di scalabilità.

L'apparato OmniSwitch 9900 è uno switch modulare layer 3 in tecnologia ASIC, equipaggiato con matrice di switching capace di erogare fino a 960 Gbps aggregati per slot e doppio alimentatore da 3000Watt. Dispone

nella parte frontale di 7 slot equipaggiabili con interfacce di rete e 4 slot per gli alimentatori, mentre nella parte posteriore equipaggia 4 slot per l'inserimento delle fabric card; include i cassetti ventole ridondati, e parti centralizzate CMM e CFM ridondate (come previsto dalla convenzione per questa tipologia di apparato). Lo chassis è predisposto per l'installazione in rack 19 pollici e occupa 11 RU. La capacità di commutazione complessiva dell'apparato offerto è pari a 2,56Tbps wirespeed.

La dotazione SW di OmniSwitch 9900 include protocolli avanzati di L3, tra cui: OSPF, BGP, IS-IS, PIM, e in aggiunta la funzionalità di Virtual Chassis, che attraverso la virtualizzazione di una coppia di apparati (visti dalla rete come un singolo apparato, con control plane, data plane e management plane unificati), consentono la realizzazione di architetture di rete in alta affidabilità, in modo semplificato.

La piattaforma OmniSwitch 9900 supporta la funzionalità IEEE 802.1AE MACsec, che consente comunicazioni sicure a livello Ethernet e IEEE 802.1aq Shortest Path Bridging per la virtualizzazione di contesti di rete (VPN).

Questi switch per la loro architettura modulare e per l'ampia gamma di schede di interfaccia equipaggiabili, si posizionano idealmente nei livelli di core nelle reti mission-critical oppure come apparato End of the Row nei Datacenter.

2.9.3. HPE Aruba 5412R zl (J9822A)

Gli switch core modulari HPE Aruba serie 5400R, appartenenti alla tipologia 9 in convenzione Consip Lan 7, offrono resilienza di classe enterprise e flessibilità innovativa nelle reti mobile-first. Questo avanzato switch modulare Layer 3 fornisce aggregazione scalabile con porte multi-gigabit HPE Smart Rate per dispositivi 802.11 AC ad alta velocità, segmentazione dinamica, tecnologia di stacking Virtual Switching Framework (VSF), failover senza disservizi, velocità di linea di 40 GbE, QoS avanzata e sicurezza, senza richiedere alcuna licenza software.

Il modello 5400R è facile da implementare e da gestire, grazie ad avanzati strumenti di sicurezza e gestione della rete quali Aruba ClearPass Policy Manager, Aruba AirWave e la piattaforma Aruba Central basata su cloud.

Il modello della serie HPE Aruba 5412R zl, presente in convenzione Consip Lan 7, per offrire alle Amministrazioni tutta la flessibilità basata sulla capacità di switching e la densità di porte necessarie dispone di 12 slot per i moduli di interfaccia ethernet.

Le componenti previste in convenzione sono:

Aruba 5400R zl2 Management Module aggiuntivo 	Aruba 5400R 700W PoE+ zl2 PSU aggiuntivo (verificare Nota a piè tabella) 
Aruba 8p 1G/10GbE SFP+ v3 zl2 Mod (half-slot) – modulo 8 porte 1/10GbE SFP+ 	Aruba 2p 40GbE QSFP+ v3 zl2 Mod (half-slot) 
Aruba 24p 1000BASE-T PoE+ v3 zl2 Mod 	Aruba 24p 1GbE SFP v3 zl2 Mod 

Nota: Per una completa alimentazione e ridondanza in qualsiasi tipo di configurazione (Slot/tipologia) Aruba consiglia l'acquisto e l'istallazione di n°4 Alimentatori.

Caratteristiche

- Potenza e innovazione per la postazione di lavoro digitale

  La serie di switch Aruba 5400R zl2 è una soluzione di accesso alla rete mobile dei campus leader del settore, con porte HPE Smart Rate multi-gigabit per una connettività ad alta velocità sui più recenti dispositivi 802.11ac (WiFI6). Offre flessibilità, sicurezza e scalabilità reali e una resilienza di classe enterprise, per le reti mobili dei campus. Basato su un ASIC ProVision di sesta generazione, Aruba 5400R dispone di un'architettura a elevata velocità e capacità con fabric switch crossbar da 2 Tbps con bassa latenza 2,1 e interfaccia API REST integrata, semplice e programmabile, che garantisce l'automazione della configurazione per le reti campus Mobile-first. Opzioni flessibili di connettività con chassis compatto a 12 slot, supporto di uplink line rate 40 GbE, fino a 96 porte line rate 10 GbE (SFP+ e 10GBASE-T), 1 GbE e fino a 288 porte di PoE+ con alimentazione interna. Software senza licenza con funzionalità avanzate Layer 2 e 3, inclusi IPv6, IPv4 BGP, routing basato su policy, VRRP, OSPF, Tunnel Node e QoS avanzata.

- Resilienza ed elevata disponibilità nell'a rete perimetrale

  La serie di switch Aruba 5400R zl2, che utilizza ProVision ASIC di sesta generazione, garantisce classificazione wire-speed e applicazione delle policy. Questo controllo degli accessi e del traffico basato su hardware assicura protezione, rilevamento e risposta alle minacce, senza compromettere le prestazioni di rete. Supporta il protocollo di ridondanza del router virtuale (VRRP) che consente a gruppi di due router di eseguire reciprocamente il backup in modo dinamico per creare ambienti di router ad alta disponibilità nelle reti IPv4 e IPv6. La ridondanza di gestione e gli impianti di alimentazione migliorano la disponibilità del sistema e la continuità operativa. I moduli hot-swap e l'alimentazione ridondante opzionale garantiscono alimentazione ininterrotta e consentono lo scambio dei moduli, senza alcun impatto sulla disponibilità della rete. Per una completa alimentazione e ridondanza in qualsiasi tipo di configurazione (numero e tipologia Slot) Aruba consiglia l'acquisto e l'istallazione di n°4 Alimentatori. Il Virtual Switching Framework (VSF) virtualizza fino a due switch fisici in un unico dispositivo logico, per offrire reti più semplici, uniformi e agili. Il rapido aggiornamento del software riduce al minimo i tempi di inattività durante l'aggiornamento su stack VSF 5400R.

- Sicurezza e qualità del servizio (QoS) efficienti e dinamiche

  La serie di switch Aruba 5400R zl2 include un set completo di funzionalità di protezione e QoS per la creazione di una rete solida, in grado di soddisfare le mutevoli esigenze aziendali in termini di criteri e conformità. Le opzioni di autenticazione flessibile includono le modalità, 802.1.x, MAC e Web per una migliore sicurezza delle applicazioni, basata su policy. Funzionalità di protezione avanzata DDOS (Distributed Denial of Service) quali DHCP Snooping, IP Source Guard e ARP Protection, nonché controlli del traffico versatili quali routing basato su criteri, QoS e ACL per la gestione delle priorità delle applicazioni end-to-end. Efficaci controlli di sicurezza con più livelli di accesso, ad esempio possibilità di

variare l'accesso alla gestione della sicurezza, RADIUS/TACACS+ e SSH per proteggere e controllare l'accesso alla gestione delle modifiche. Proteggete la periferia della vostra rete IPv6 con DHCPv6 Protection e blocco Dynamic IPv6. Tunnel Node per trasportare il traffico di rete al controller Aruba, con autenticazione e policy di rete applicate e imposte a livello di controller

- Semplifica la gestione integrata cablata o wireless

  La serie di switch Aruba 5400R zl2 supporta ClearPass Policy Manager per una policy unificata e costante tra utenti cablati e wireless, semplificando l'implementazione e la gestione dell'accesso guest, l'accettazione degli utenti, l'accesso alla rete, la sicurezza, la QoS e altre policy di rete. Supporta il software Aruba AirWave, che fornisce una piattaforma comune per la gestione del provisioning zero-touch e il monitoraggio per dispositivi di rete cablati e wireless.

2.9.4. Huawei 7706

Il modello 7706 è uno switch modulare da 10 RU della series S7700 adatto al mondo Campus come elemento di aggregazione ma anche come nodo di MAN e di Core con supporto di funzionalità MPLS (e relative applicazioni L2/3 VPN), e schede di linea con supporto della Full Internet Routing Table (FIB da 3M di entry).

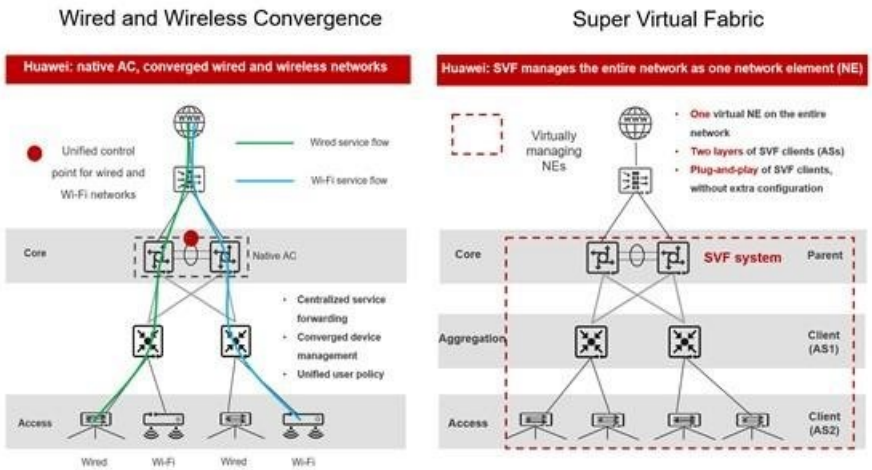
È in grado di supportare altissime scalabilità in termini di porte (36x100GE/36x40GE/288x10GE/GE), interfacce fino a 100GE e capacità di switching fino a 3.84 Tbit/s con un throughput complessivo di 2880 Mpps. Ha 8 slot: 6 per equipaggiare le opportune schede di linea e i 2 centrali riservati alle Switching Routing Unit (SRU) che operano in modalità backup o load-balancing e permettono di avere una capacità di switching di 720Gbps per slot.

È ridondato in tutte le sue componenti: alimentazione con 4 moduli da 3000W, doppio modulo di ventole (ognuno con doppia ventola), doppia SRU che opera da control e forwarding plane (matrice di commutazione) per il traffico delle schede attestate. Inoltre, la macchina implementa la tecnologia di Clustering Switching System (CSS) che consente di aggregare 2 dispositivi fisici in un singolo chassis logico con semplificazione dell'operatività e della topologia di rete. Il Clustering è possibile realizzarlo anche in modalità long distance, con i 2 apparati in 2 CED distinti e interconnessi opportunamente.

Oltre alle piene funzionalità di switching e di routing avanzato, network overlay, multicast e MPLS tipiche di uno switch di Core e Aggregazione, il 7706 opera da Wi-Fi Controller attraverso l'equipaggiamento delle schede presenti nella Convenzione, realizzando quindi una convergenza tra dominio Wired e Wireless.

Le schede in dotazione permettono un'alta scalabilità e dorsali da 40G e 100G: schede con 6 porte dual rate 40GE o 100GE e 48 porte dual rate 10G (lavorano anche a 1Gbps).

In aggiunta, attraverso la tecnologia di virtualizzazione SVF (Super Virtual Fabric), di concerto ai modelli di accesso (Tipo 1-5), è possibile virtualizzare una rete a 2 strati in cui Aggregazione e switch di Accesso e Wi-Fi Access Point sono visti come un unico switch logico semplificando il management della rete, la configurazione e il monitoraggio dei servizi dall'elemento di Aggregazione e permettendo di dispiegare gli switch di accesso in modalità plug-and-play (alla stessa stregua di un AP controllato da un Wi-Fi Controller).



È gestibile (configurazione, monitoraggio e allarmistica) dal sistema di management eSight (Tipo 10) incluso all'interno della Convenzione.

2.9.5. ZTE 8905E-CMP3A-AC2

Gli switch ZXR10 serie 8900E sono switch di core modulari di fascia alta con grande capacità di switching, piena capacità L2/L3/MPLS, alte prestazioni, affidabilità e sicurezza avanzate e fino a 10.24Tbps di capacità con interfacce GE/10GE/40GE/100GE. La tecnologia VSC è in grado, inoltre, di fornire un solido cloud core. Le capacità multi-service bearing e il meccanismo multidimensionale di sicurezza e affidabilità garantiscono servizi sempre online. Gli apparati posseggono funzionalità complete IPv6 e MPLS. Gli switch della serie ZXR10 5960-H supportano le seguenti ulteriori funzionalità:

- VSC (Virtual Switch Cluster) 2.0: Fino a 4 apparati sono visti, logicamente, come un unico apparato;

- ZESR – ZTE Ethernet Smart Ring network technology: algoritmo di protezione di un anello in fibra in 10ms;
- Service Quality Analyzer: lo switch è in grado di inviare pacchetti ad un server per misurare la qualità della linea;
- Zero-touch provisioning: caricamento della prima configurazione tramite Stick USB;

Il modello proposto è: 8905E (layer 3 – Modulare small). L'apparato comprende n° 5 slot per le schede di linea, 2 switching control board e doppia alimentazione con una dimensione di 10 RU. La capacità di switching è di 6.4 Tbps. L'apparato è gestibile dal sistema di management NetNumen, incluso all'interno della Convenzione (Tipo 10).

2.10. Switch Tipo 10

2.10.1. Juniper Junos Space Network Director

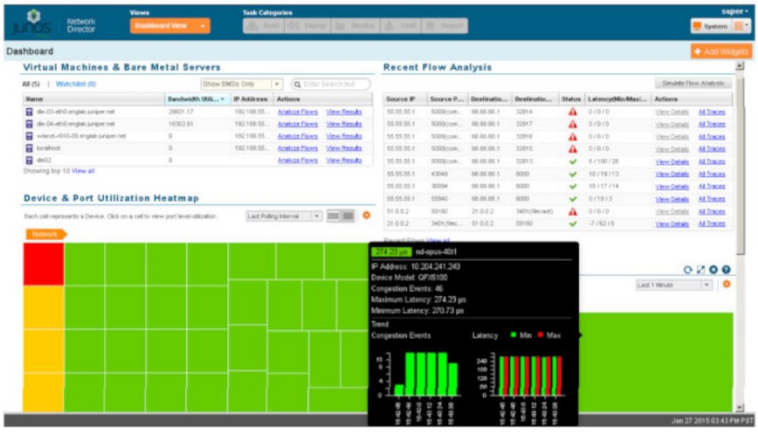
Junos Space e Junos Space Network Director è una soluzione software di Network Management che include funzionalità di visualizzazione, analisi e gestione di reti Enterprise in ambito campus lan e data center.

Junos Space Network Director fornisce un'unica console di gestione che permette di accedere alle funzioni di gestione, automazione e provisioning della piattaforma, che è costituita da tre componenti software principali:

- Junos Space Network Management Platform: fornisce tutte le funzioni tipiche di una piattaforma FCAPS (fault, configuration, accounting, perfomance and security);
- Junos Space Management Applications – applicazioni domain-specific che forniscono le funzionalità' di configurazione e provisioning dei servizi di rete sugli apparati Juniper Networks;
- Junos Space SDK (software development kit) – una soluzione di programmazione per integrare l'infrastruttura di rete nei processi e nelle applicazioni aziendali.

Funzionalità in evidenza

Device Discovery	Strumento Wizard based per il discovery degli apparati di rete
Topology	Vista topologica dell'infrastruttura a diversi livelli
Inventory	Gestione degli asset relativi all'infrastruttura di rete
Software image	Gestione centralizzata delle release software
Configuration Template	Template per la gestione della configurazione degli apparati di rete
Configuration Management	Gestione avanzata dei file di configurazione: import, export, compare, backup/restore, scheduling
Fault and Performance	Eventi e performance management per tutta l'infrastruttura di rete



2.10.2. ALE OmniVista 2500

Alcatel-Lucent Enterprise OmniVista® 2500 è Il sistema di gestione (NMS) che fornisce strumenti per la gestione, il provisioning, il monitoraggio e la visibilità a livello di rete, per aumentare l'efficienza IT e l'agilità aziendale. Dispone di un set completo di funzionalità di gestione secondo il modello FCAPS (fault, configuration, administration, performance, security), in modo unificato, sia per la componente LAN che Wireless LAN dell'infrastruttura di rete.

Questa piattaforma consente agli amministratori di rete di semplificare le attività di gestione dell'intera infrastruttura con i suoi elementi di rete, gli allarmi, i criteri di sicurezza di accesso e di virtualizzazione.

Eroga funzioni di analisi di rete per una visibilità completa su dispositivi di rete cablati, wireless, endpoint IoT e applicazioni, così come l'analisi predittiva per il supporto di logiche di pianificazione anticipata.

OmniVista 2500 è una soluzione completa per gestire e monitorare la rete LAN e Wireless LAN ed è accessibile da qualsiasi dispositivo munito di browser mediante una interfaccia grafica Web 2.0, che si adatta alle dimensioni dello schermo del dispositivo utilizzato.

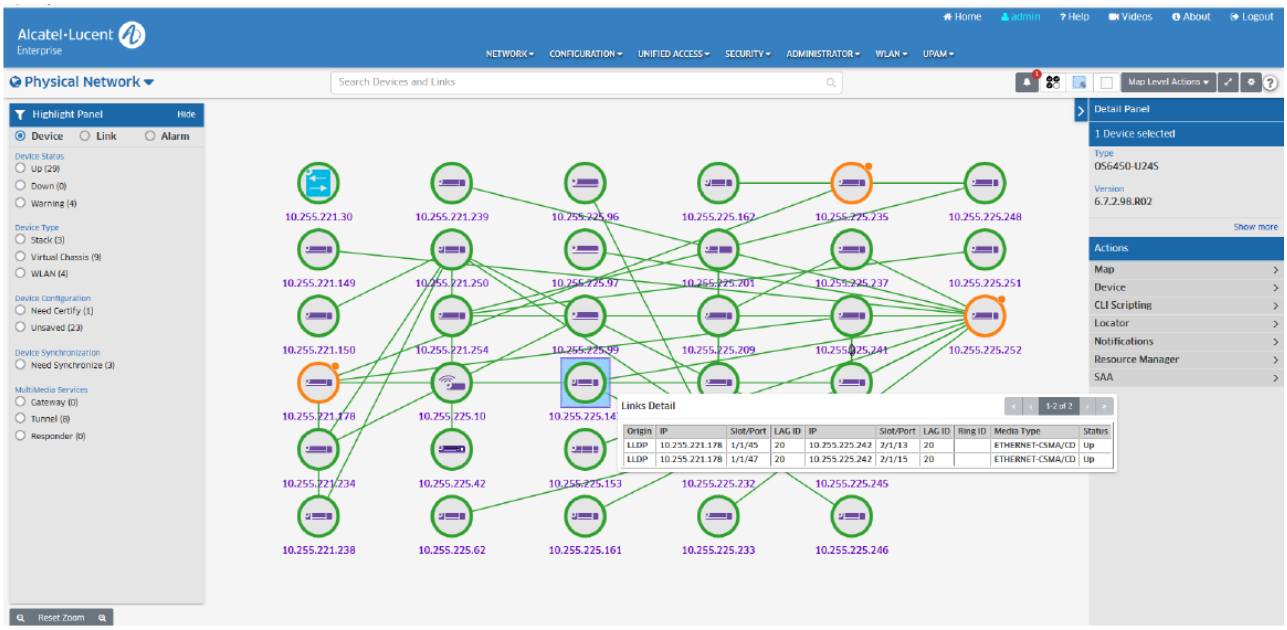
Tra le principali funzionalità disponibili evidenziamo:

Cruscotto Personalizzabile

- Monitoraggio e analisi in tempo reale degli indicatori critici delle prestazioni di rete attraverso widget visivi per LAN e punti di accesso Stellar Punti di accesso wireless Stellar;
- Configurazione personalizzabile dei widget da visualizzare nel cruscotto, ad esempio dati e altre importanti informazioni sulla rete e sui dispositivi cablati e wireless.

Network discovery

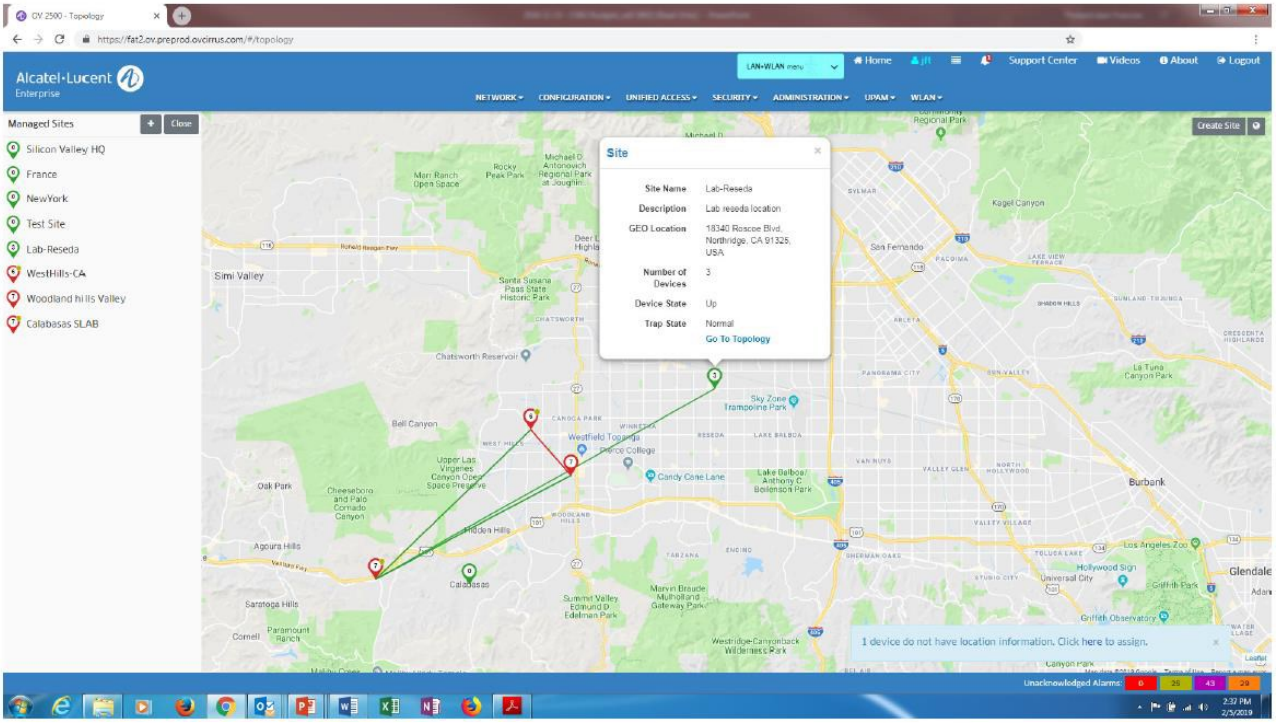
- Individuazione dettagliata di apparati Alcatel-Lucent Enterprise e dispositivi di terze parti mediante SNMPv2c/v3;
- Registrazione degli Access Point Stellar con configurazione completa dei servizi wireless.



Topologia

- Integrazione della mappa di Google visualizzando i dispositivi o i siti della rete in base all'indirizzo della sua posizione fisica o in base alle sue coordinate GPS;
- Visualizzare l'elenco dei dispositivi, lo stato delle apparecchiature associate a un sito geografico;
- Layout gerarchico della mappa per infrastrutture con elevato numero di nodi;
- Visualizzazione logica e fisica della rete, con informazioni effettive sulle adiacenze e sullo stato dei dispositivi;
- Viste per sottoreti IP, protocollo ITU G.8032 ERP, protocollo SPB-M;

- Mappa logica dinamica, personalizzabile, basata su filtri definiti dall'utente (subnet IP, posizione, modello di dispositivo, informazioni descrittive fornite dall'utente, mappe personalizzate).



Gestore Allarmi

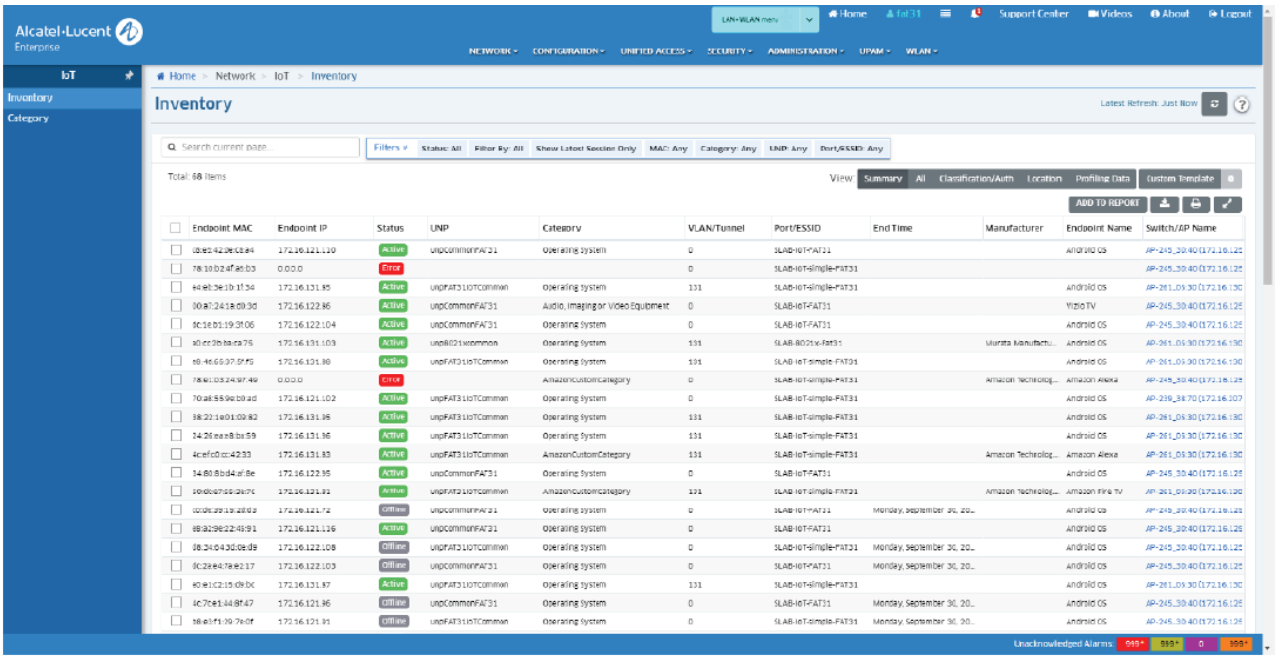
- Monitora e analizza gli avvisi e le notifiche generati della rete (Apparati Alcatel-Lucent e dispositivi di terze parti in tempo reale;
- Funzionalità di notifica avanzate attraverso filtri personalizzabili e ordinamento per severity;
- Azioni di notifica verso piattaforme esterne basate su condizioni predefinite con un solo clic.

Localizzatore

- Rapida risoluzione dei problemi e isolamento dei problemi di rete con un solo clic;
- Consente agli amministratori di cercare e individuare rapidamente la posizione del dispositivo e i dispositivi associati, in base a più criteri come ad esempio ricerche in tempo reale o storiche;
- Individua i dispositivi di terze parti e indica il dispositivo Alcatel-Lucent Enterprise più vicino, mostrando il collegamento su una mappa topologica;
- Accelera la risoluzione dei problemi con il menu contestuale del tasto destro del mouse e l'interazione diretta con altri componenti del sistema OmniVista 2500.

Analisi di rete

- Fornisce informazioni sullo stato della rete con analisi grafiche avanzate sui dispositivi più problematici in base allo stato del dispositivo (CPU, memoria, temperatura);
- Monitora la larghezza di banda della rete e i modelli di traffico fino al livello della porta del dispositivo attraverso la raccolta di statistiche sflow®;
- Fornisce informazioni sulle applicazioni che stanno consumando la maggior parte della larghezza di banda (Top N apps), monitora il traffico delle applicazioni utilizzate dagli utenti (Top N talkers), e memorizza e visualizza i dati di flusso con una granularità fino a un minuto;
- Fornisce informazioni sulla salute della rete con un'analisi grafica avanzata sugli switch più problematici basata sullo stato del dispositivo (CPU, memoria, temperatura) e sull'erogazione PoE (Power over Ethernet);
- Aiuta gli amministratori di rete a comprendere in anticipo potenziali problemi di congestione di rete, analizzando l'utilizzo delle applicazioni sulle porte e potenziali anomalie di utilizzo, che potrebbero pregiudicare il corretto funzionamento e le prestazioni della rete, consentendo così una migliore esperienza dell'utente finale;
- Supporta l'inventario dei dispositivi IoT rilevati mediante la funzionalità di fingerprinting degli endpoint, offrendo all'amministratore di rete la piena visibilità di tutti i dispositivi connessi sulla rete (LAN e Wireless LAN) con informazioni contestuali complete, tra cui attributi chiave come il tipo di dispositivo, il fornitore, versione dell'hardware, posizione della rete e informazioni sul tempo di connessione.



Configurazione della fabric

- Provisioning semplificato del protocollo Shortest Path Bridging (SPB-M) attraverso interfaccia grafica seguendo tutti i passaggi di configurazione necessari per definire e selezionare i dispositivi che fanno parte della dorsale SPB e successivamente creare tutti i parametri di base e avanzati del servizio (ISID,

SAP, BVLAN) attraverso un flusso di lavoro One-Touch, riducendo la complessità e il tempo per il roll-out dell'infrastruttura di rete;
- Visualizzazione e monitoraggio del protocollo Shortest Path Bridging (SPB-M) dall'applicazione di Topology, compresa la visualizzazione dei dispositivi configurati SPB-M, lo stato dei servizi configurati sui dispositivi che costituiscono la fabric (SDP e SAP).

Gestione delle risorse

- Gestisce il ciclo di vita completo della configurazione del dispositivo (backup, ripristino);
- Supporta routine di automazione degli aggiornamenti dell'immagine software per tutta l'infrastruttura di rete (Access Point Stellar e OmniSwitch).

Provisioning basato su template

- Implementazione automatica di politiche di provisioning coerenti e configurazione dei dispositivi;
- Consente di effettuare il provisioning dei dispositivi OmniSwitch off the-shelf semplicemente collegandosi alla rete;
- Applica la golden-configuration e le best practice monitorando la conformità mediante audit.

Autenticazione con regole unificate

- Autenticazione con criteri unificati su base ruolo per utenti cablati e wireless;
- Strategia di autenticazione flessibile con configurazione semplificata per la definizione del profilo dell'utente finale che consente diritti di accesso alla rete appropriati e politiche aziendali dinamiche;
- On-boarding del client IPv6, compresa l'autenticazione e l'autorizzazione, che estende i criteri di accesso unificato.

L'offerta in Convenzione comprende il Software OmniVista 2500 sotto forma di Virtual Appliance corredato di pacchetti di licenze dimensionate su tre diverse fasce (come da richiesta di capitolato):

- OV2500-100-N: OmniVista 2500 + licenze per la gestione di fino a 100 nodi di rete (LAN e/o WiFi);
- OV2500-500-N: OmniVista 2500 + licenze per la gestione di fino a 500 nodi di rete (LAN e/o WiFi);
- OV2500-1000-N: OmniVista 2500 + licenze per la gestione di fino a 100 nodi di rete (LAN e/o WiFi).

Licenza di gestione dei nodi LAN

Le licenze di gestione della rete forniscono la gestione dei dispositivi per il provisioning avanzato, monitoraggio e analisi per i dispositivi ALE, compresa la visibilità delle applicazioni e gli aggiornamenti delle firme per Alcatel-Lucent OmniSwitch® 6860E/6860N series. Una licenza include la gestione dei nodi di terze parti, come il rilevamento, la topologia e la risoluzione dei problemi per il protocollo Simple Network Management (SNMP) di terze parti.

Licenza di gestione degli Access Point Stellar

Le licenze per gli access point forniscono una gestione unificata per la serie Alcatel-Lucent OmniAccess Stellar. Le licenze includono operazioni di gestione unificata della rete come la registrazione del punto di accesso, la topologia, il monitoraggio, il ciclo di vita convergente, la visibilità delle applicazioni e la definizione unificata dei ruoli. Sono incluse le funzionalità specifiche della componente wireless LAN come la gestione RF, Heatmap, WiPS (Wireless Intrusion Prevention System).

La soluzione offerta in Convenzione non comprende server HW: Per il dimensionamento e la scelta della componente server suggeriamo di consultare le specifiche disponibili nel datasheet scaricabile al seguente link:

https://www.al-enterprise.com/-/media/assets/internet/documents/omnivista-2500-nms-datasheet-en.pdf

2.10.3. HPE Aruba – AirWave (AW-100C - AW-500C - AW-1000C)

Aruba AirWave è un sistema di gestione di rete potente e di facile utilizzo, che non solo supporta solo l'infrastruttura cablata e wireless di Aruba, ma anche di una vasta gamma di altri produttori. Fornisce una visibilità granulare su dispositivi, utenti e applicazioni della rete. Con un'introspezione senza precedenti e un controllo centralizzato per gestire in modo efficace le infrastrutture aziendali globali, AirWave consente alle organizzazioni IT di ottimizzare in modo proattivo le prestazioni della rete, rafforzare la sicurezza wireless, e migliorare l'esperienza dell'utente finale.

Attraverso un'interfaccia utente centralizzata e intuitiva, AirWave fornisce monitoraggio in tempo reale, avvisi proattivi, report storici e risoluzione dei problemi rapida ed efficiente. Le visualizzazioni di pannelli dedicati consentono di visualizzare rapidamente potenziali problemi di copertura radiofrequenza (RF), traffico di comunicazioni unificate e di collaborazione (UCC), prestazioni delle applicazioni e integrità dei servizi di rete.

Il modulo aggiuntivo Aruba Clarity analizza in modo proattivo la qualità dell'esperienza degli utenti finali fornendo funzionalità di monitoraggio avanzate per servizi di rete critici, come guasti e tempo di risposta per un dispositivo mobile nell'associazione a una componente radio Wi-Fi. Altri servizi monitorati includono il tempo di autenticazione attraverso un server RADIUS, la raccolta di un indirizzo IP tramite server DHCP, e la risoluzione dei nomi per i servizi DNS. Ciò consente alle organizzazioni IT di visualizzare la visibilità end-to-end dei problemi prima che scalino, mentre le metriche vengono monitorate in tempo reale e acquisite anche tramite test opzionali a richiesta, o pianificati per analisi predittiva.

AppRF fornisce una visibilità approfondita sulle applicazioni e sul traffico Web in rete, per garantire che le app mission-critical ottengano priorità, che gli utenti non visitino siti rischiosi, o anche solo misurare i modelli di utilizzo. Un pannello UCC dedicato offre una visibilità granulare delle applicazioni di Unified Communications come Skype for Business e tutte le chiamate Wi-Fi che attraversano la rete.

La posizione e la mappatura di VisualRF offrono viste a livello di rete dell'intero ambiente RF. Le mappe della copertura Wi-Fi e la sottostante topologia cablata mostrano un'immagine chiara e precisa di chi si trova sulla rete, posizione e rendimento dei componenti. Inoltre, gli overlay dello stato dei client, e le prestazioni delle

applicazioni, possono aiutare a diagnosticare rapidamente problemi specifici per un client, una planimetria, o un percorso specifico. Il rilevamento rogue AirWave RAPIDS funziona attraverso un modulo software di protezione dalle intrusioni wireless denominato RFProtect, per raccogliere dati e mitigare i problemi con AP rogue, client non autorizzati e eventi di intrusione wireless su reti cablate e wireless. I dati wireless raccolti da RAPIDS sono correlati con i dati della rete cablata per identificare le minacce più significative e rilevanti, riducendo al contempo i falsi positivi e rafforzando la sicurezza della rete.

Disponibile come software o dispositivo hardware e software combinato, AirWave offre all'IT la possibilità di prendere decisioni intelligenti e ben informate sulla rete, riducendo al tempo stesso i costi e la complessità del miglioramento della qualità del servizio.

In convenzione sono disponibili i seguenti pacchetti di licenze, che sarà possibile acquistare in base alle proprie esigenze:

Software per la gestione fino a **100 nodi**	HPE Aruba Airwave include RAPIDS and VisualRF (100 Nodi) e comprensivo di sw di virtualizzazione	**AW-100C**
Software per la gestione fino a **500 nodi**	HPE Aruba Airwave include RAPIDS and VisualRF (500 Nodi) e comprensivo di sw di virtualizzazione	**AW-500C**
Software per la gestione fino a **1000 nodi**	HPE Aruba Airwave include RAPIDS and VisualRF (1000 Nodi) e comprensivo di sw di virtualizzazione	**AW-1000C**

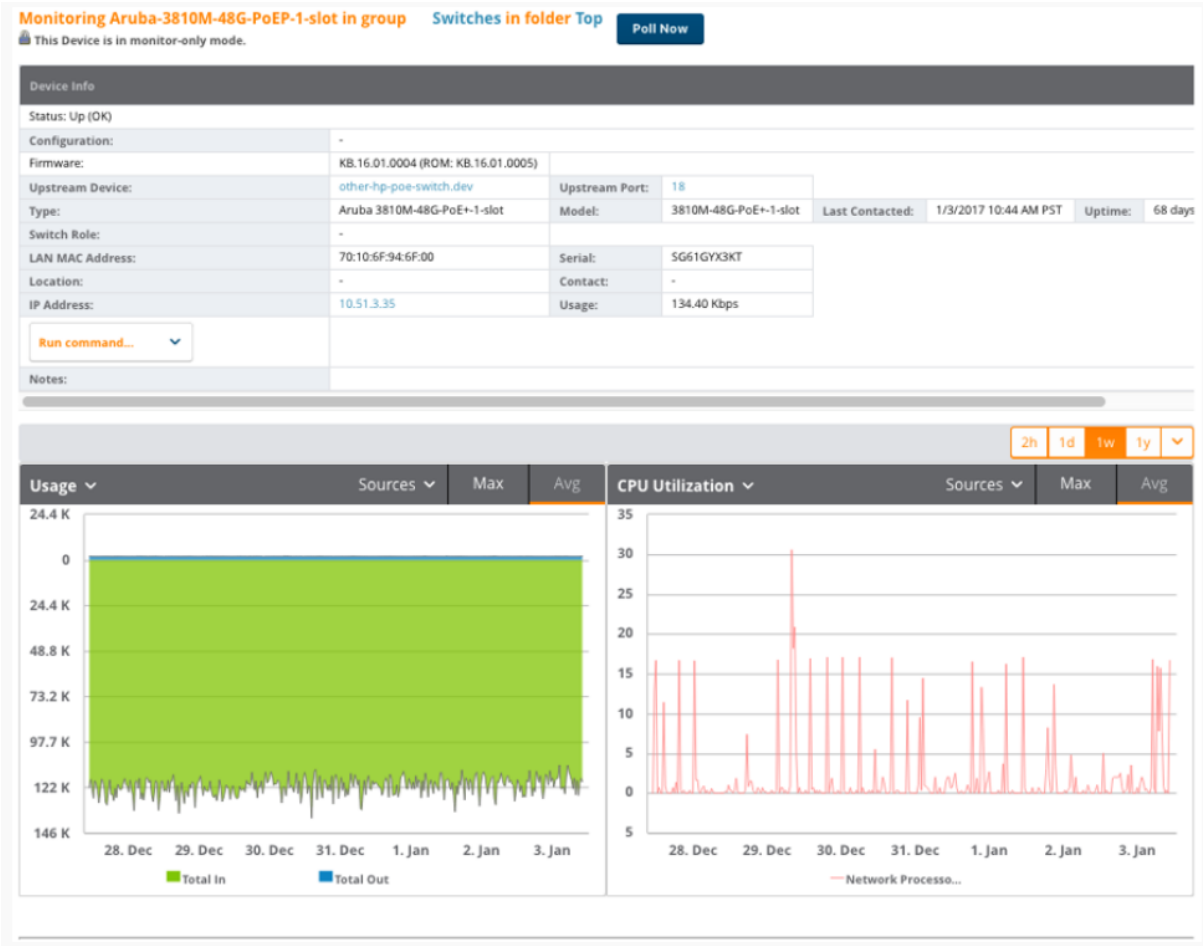
RISOLVI I POBLEMI DI CONNETTIVITÀ PRIMA CHE SI VERIFICHINO

Con il nuovo modulo Aruba Clarity, AirWave monitora proattivamente le metriche critiche non RF: il tempo necessario a un dispositivo mobile per associarsi a una radio Wi-Fi, autenticarsi su un server RADIUS, raccogliere un indirizzo IP tramite DHCP o risolvere nomi per Servizi DNS. Con avvisi personalizzati e test del cliente simulati, Clarity consente all'IT di intraprendere azioni proattive contro i problemi di prestazioni futuri.

MONITORAGGIO E VISIBILITÀ IN TEMPO REALE

- Visualizzare automaticamente tutti gli utenti e i dispositivi: wireless e remoti - sulla rete.
- Misurare i tempi di risposta e i tassi di errore per client, associazione con radio Wi-Fi, autenticazione con Server RADIUS, tempi di risposta DHCP, e risoluzione DNS.
- Monitorare l'infrastruttura cablata che collega il wireless controller e AP.

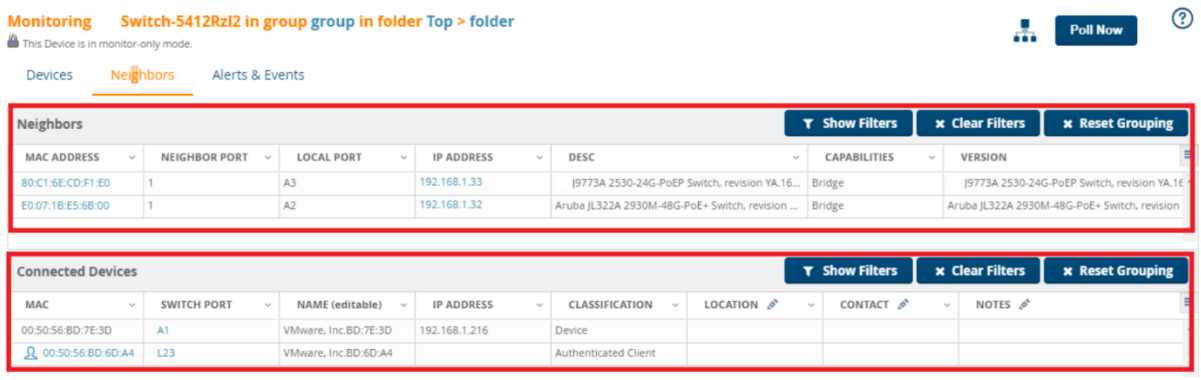
- Visualizza errori radio, tra cui rumore di fondo e informazioni sull'utilizzo del canale, cause frequenti di problemi di connettività.
- Analizza da livello di rete a livello di dispositivo monitoraggio delle visualizzazioni.
- Memorizza e visualizza le prestazioni, la capacità e statistiche a livello di applicazione, traffico Web e rete deviazioni per un periodo di 40 settimane.



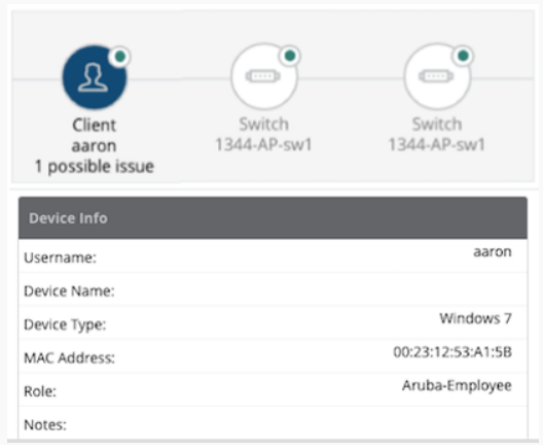
Gli avvisi sui dispositivi aiutano gli amministratori a tenere traccia degli eventi principali come il mancato collegamento, il riavvio dei dispositivi, il mancato funzionamento dell'alimentazione o altri eventi che possono avere un effetto significativo non solo sul dispositivo stesso ma anche sulla rete.

Visibilità dei client connessi alla rete cablata

AirWave fornisce i dati per aiutare gli amministratori di rete ad identificare gli switch adiacenti, nonché i client autenticati e non autenticati collegati a uno switch. Ciò è di grande aiuto per comprendere i peer dello switch nonché i client che dipendono da un particolare switch. La mappatura dei client collegati allo stato della porta, alla potenza consumata e alla priorità PoE è utile per identificare potenziali problemi prima che si verifichino.



Inoltre, per i client autenticati, sono disponibili dettagli come nome utente, VLAN, indirizzo IP e ruolo utente:

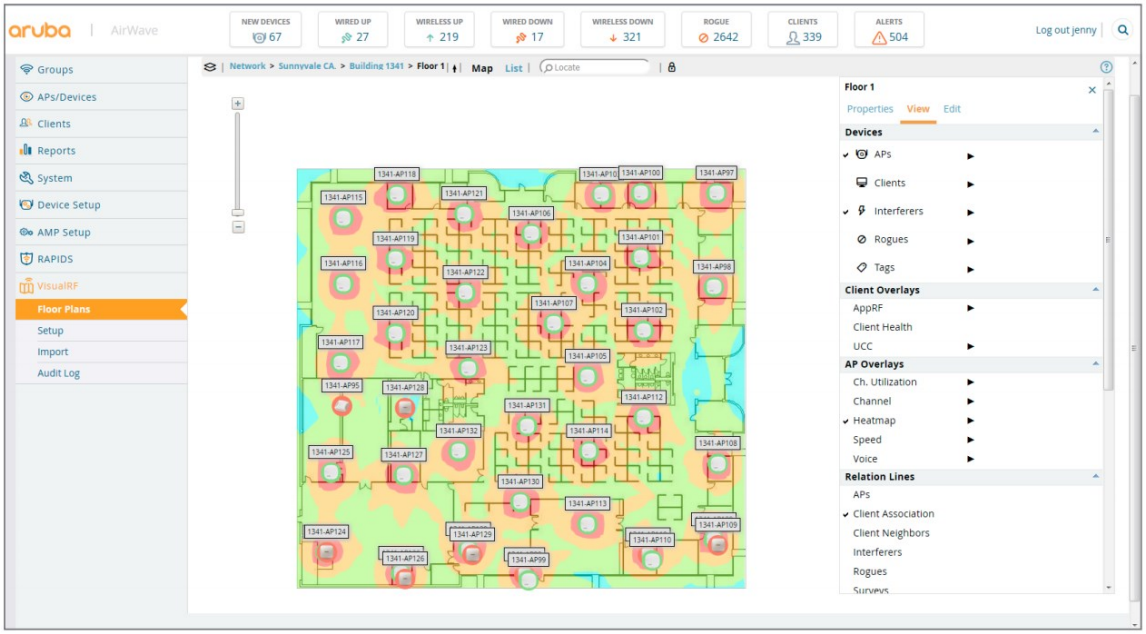


APPRF

Per una visibilità approfondita delle applicazioni e del traffico web, AppRF assicura che le app mission-critical abbiano la priorità. È possibile valutare l'utilizzo complessivo delle applicazioni, e avere visibilità sugli utenti che inducono le maggiori quote di traffico. Una dashboard UCC dedicata offre una visibilità granulare per applicazioni di comunicazioni unificate come Skype per Business e tutte le chiamate Wi-Fi che attraversano la rete.

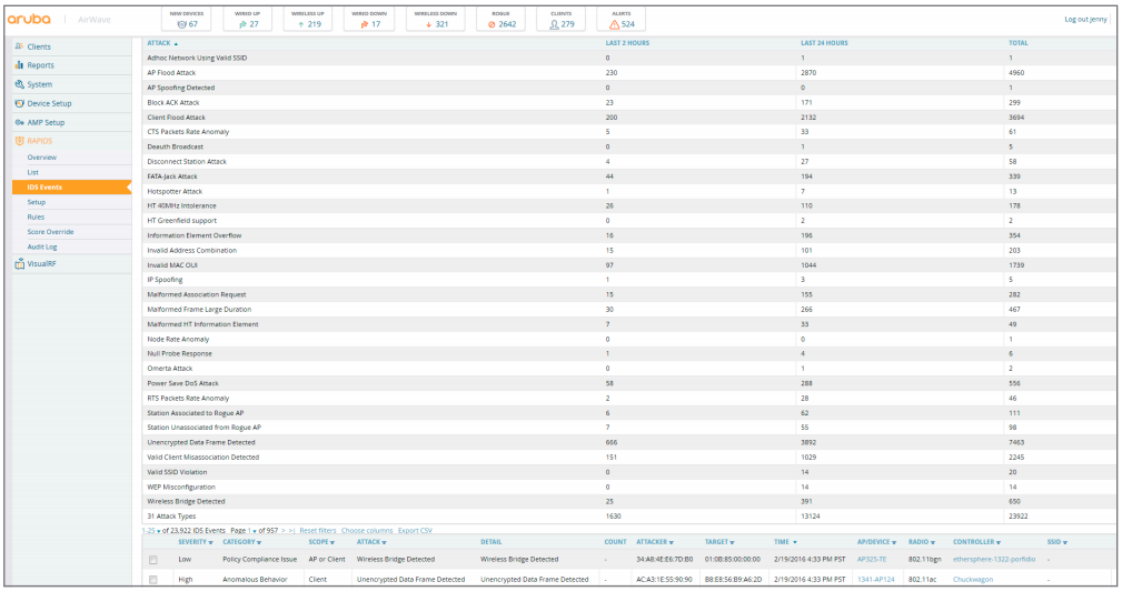
VISUALRF

I servizi di localizzazione e mappatura delle posizioni offrono viste dell'intero ambiente RF. Mappe di copertura Wi-Fi, e della sottostante topologia cablata, mostrano un'immagine chiara e accurata di chi è sulla rete, posizione, e comportamento generale della rete. Le sovrapposizioni configurabili mostrano lo stato e delle applicazioni dei client con relative prestazioni, per diagnosticare rapidamente problemi specifici per ogni client, per una mappa specifica, per un intero piano, o posizione specifica.



RAPIDS

Il rilevamento rogue AP di AirWave funziona con il modulo Aruba RFProtect, con protezione dalle intrusioni wireless e raccolta dati per attenuare i problemi dovuti a rogue AP e client, eventi di intrusione wireless e wired. I dati wireless raccolti sono correlati con la rete dati per identificare le minacce più significative e rilevanti, riducendo notevolmente i falsi positivi e aumentando significativamente il rafforzamento complessivo della sicurezza della rete.



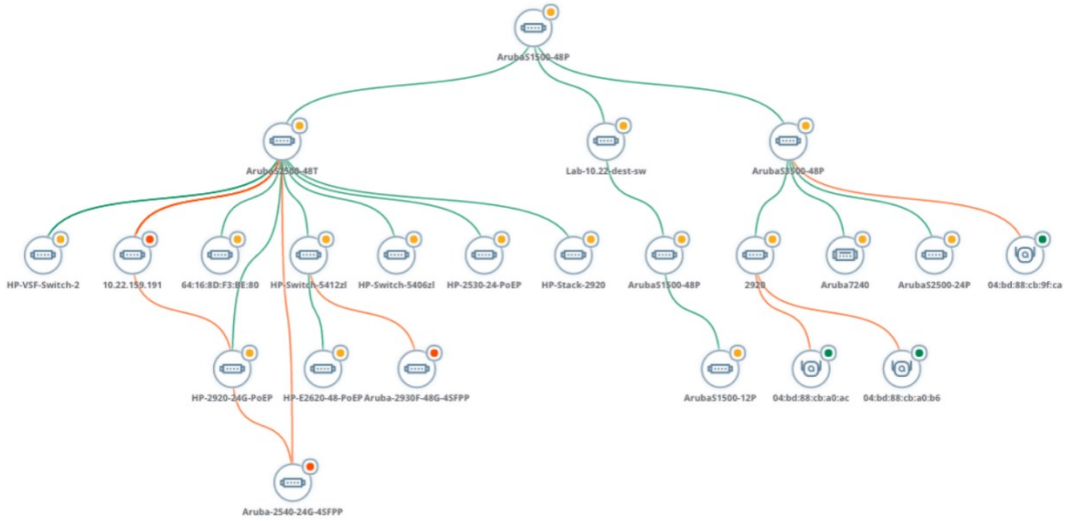
DISCOVERY DISPOSITIVI

- Rileva automaticamente e mappa i dispositivi dell'intera infrastruttura, sia essa infrastruttura WLAN o Wired

- Funziona in qualsiasi ambiente di rete, inclusi quelli di grandi dimensioni e su reti distribuite multi-sito.
- Mostra la relazione tra AP, controller e switch al fine di produrre una topologia della rete

Vista della Topologia

AirWave rileva, identifica e crea automaticamente una topologia in tempo reale dell'intera rete; in particolare, in una rete mista wired e wireless, la piattaforma è in grado di creare una mappa dell'ambiente RF e della topologia cablata sottostante. La topologia può anche includere dispositivi di altri fornitori, purché gli altri dispositivi utilizzino un protocollo basato su standard come LLDP per annunciarsi.

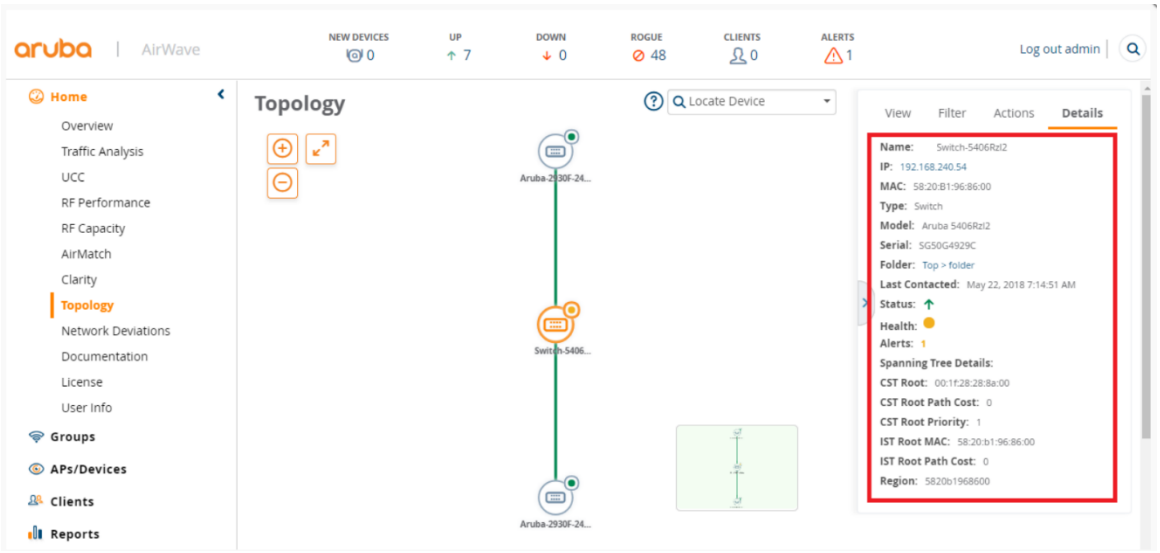


La topologia mostra

- la connettività L2
- l'integrità dei dispositivi
- i collegamenti che li interconnettono e consente inoltre di individuare un dispositivo tramite il numero di modello
- il tipo di dispositivo
- la cartella in cui è stato configurato.

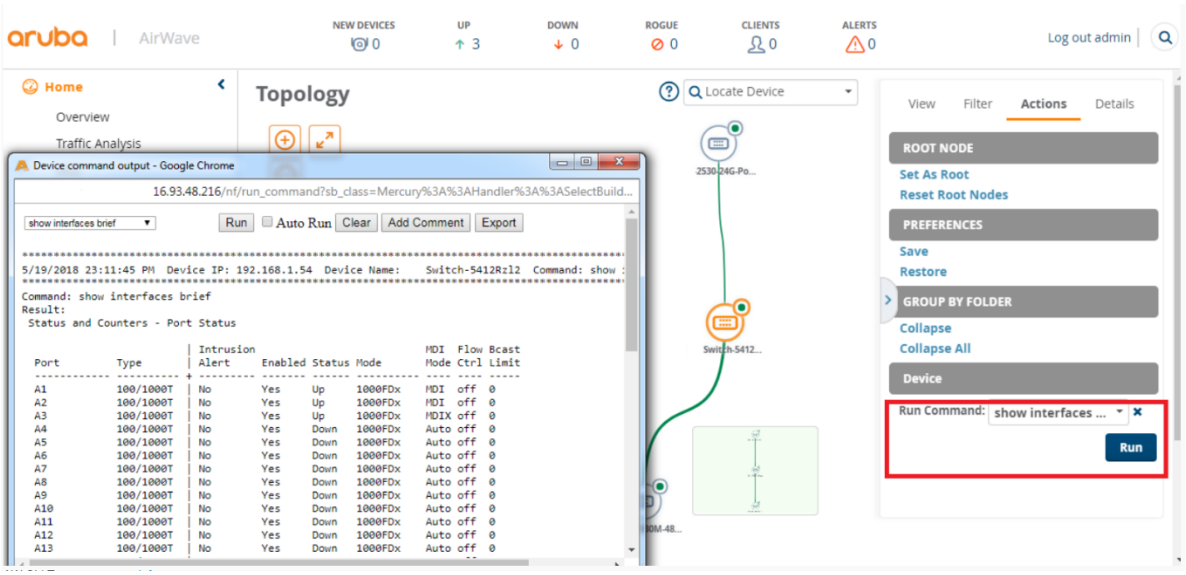
Facendo clic su di un determinato dispositivo nella topologia vengono inoltre forniti i dettagli di quel particolare dispositivo (inclusi modello, numero di serie, stato di salute, avvisi e dettagli STP).

Facendo clic invece su un collegamento nella topologia vengono forniti dettagli sullo stato di salute, la velocità e il tipo di collegamento, compreso il suo stato di aggregazione (LACP).



La vista "Topologia" consente inoltre agli amministratori di cercare ed evidenziare una parte della rete per VLAN e per Spanning Tree. Questo può essere utile per restringere il campo a una particolare porzione della rete senza distrarsi, specialmente nelle reti di grandi dimensioni.

Per comodità, i comandi CLI possono essere eseguiti anche direttamente dalla vista "Topologia". Ad esempio, l'esecuzione di "show interfaces brief" può mostrare i dettagli della porta e quindi un amministratore può comprendere meglio il motivo di un eventuale avviso.



RISOLUZIONE DEI PROBLEMI E DIAGNOSTICA

- Visualizza i dati di dispositivi client ArubaOS, Instant e ClearPass Policy Manager; comprendendo incluso il tipo di dispositivo, il sistema operativo, dettagli del sistema operativo, produttore e modello.
- Ricerca di client per nome utente o indirizzo MAC, visualizzazione diagnostica delle statistiche dei dispositivi di rete, unitamente ad indicatori per valutare lo stato di salute e le prestazioni complessive.

- Sovrapposizione dello stato dei client su planimetria per diagnosticare problemi specifici per client o su un'area della mappa.
- Diagnostica facilmente problemi di radiofrequenza

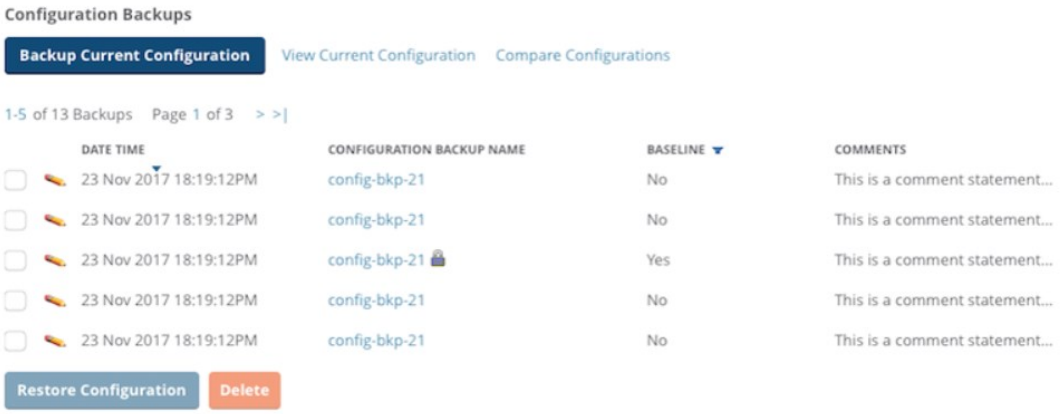
ANALISI DELLA CAUSA E CORRELAZIONE EVENTI

- Mappa le relazioni tra gli AP controller e switch per identificare principali cause dei tempi di inattività e problemi di prestazioni.
- Correla i problemi di prestazioni e tempi di inattività in modo tale da inviare singoli avvisi di allarme.

GESTIONE DELLE CONFIGURAZIONI

- Configura automaticamente AP, controller, Aruba Instant, e Aruba Switches.
- Permette di definire le politiche di configurazione attraverso un'interfaccia utente web, o importando una configurazione nota da un dispositivo esistente.
- Configura gli AP Instant Aruba facilmente in ambienti multi-sito.
- Permette di eliminare dispendiosi ed inclini ad errori operazioni ed aggiornamenti manuali per mezzo di una efficiente distribuzione del software remoto.
- Supporta aggiornamenti avanzati del firmware con possibilità di scelta ed imposizione versioni certificate, con download differiti di immagini e processi di riavvio, nonché supporto per la programmazione posticipata degli aggiornamenti o delle modifiche del firmware.
- Archivia configurazioni dei dispositivi ed esegue e backup dei flash per ripristinare le statistiche e le configurazioni precedenti dei controller Aruba.
- Mantiene registri di verifica dettagliati delle modifiche apportate da tutti gli operatori di AirWave.

La modifica della configurazione è un evento importante e deve essere monitorata attentamente per correlare la modifica del comportamento della rete alla modifica della configurazione stessa. AirWave può eseguire backup periodici dei dispositivi, eseguire automaticamente controlli di configurazione e avvisare gli amministratori nel caso in cui la configurazione del dispositivo sia diversa da quella che AirWave si aspetta che sia.



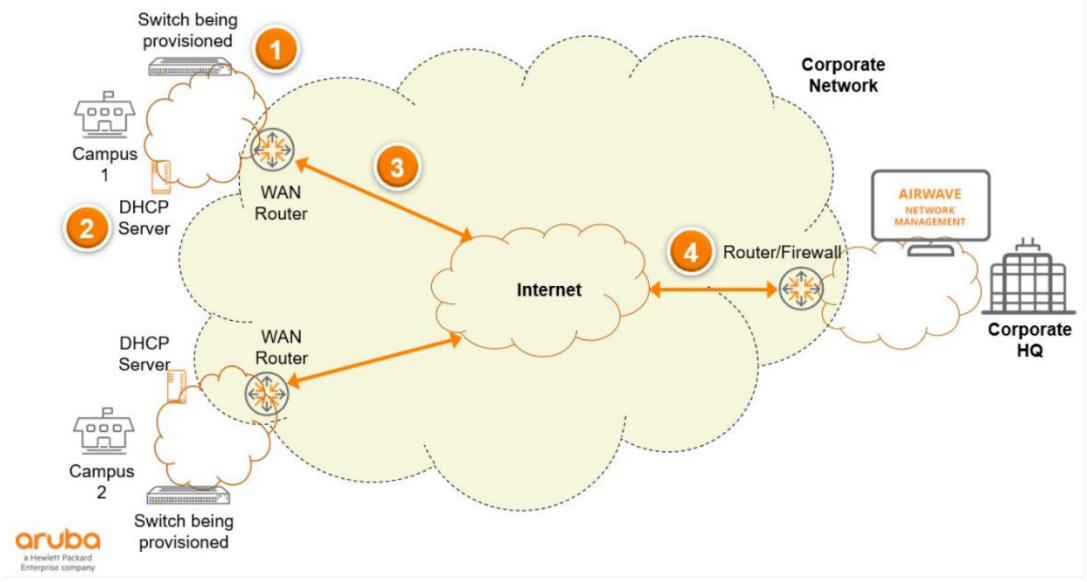
Per questo motivo, AirWave esegue backup periodici dei dispositivi in modo che l'amministratore possa scegliere di ripristinare l'ultima configurazione funzionante nota nel caso in cui lo stato della rete non sia quello previsto oppure se qualcuno modifica accidentalmente la configurazione all'insaputa dell'amministratore.

Zero Touch Provisioning

La funzionalità di Zero Touch Provisioning utilizza template di configurazione che permettono di automatizzare tutto il processo di configurazione e di deployment per aziende distribuite che devono gestire anche gli uffici e le sedi remote.

Lo ZTP garantisce che, una volta che la configurazione per un tipo di dispositivo è resa disponibile su AirWave, la configurazione dello switch possa avvenire in modo asincrono senza la necessità che un amministratore di rete sia presente presso la sede centrale o il campus al momento del deployment, riducendo così i tempi, i costi e il personale necessari per la gestione delle filiali remote eliminado allo stesso tempo anche eventuali errori umani di configurazione.

ZTP è disponibile solo per i dispositivi Aruba; i dispositivi di fornitori di terze parti possono essere rilevati avviando scansioni di rete o caricando un file CSV su AirWave. In un ambiente multi-vendor, gli utenti possono scegliere uno di questi metodi per rilevare i dispositivi e inserirli nelle cartelle AirWave appropriate per inviare automaticamente la configurazione a quei dispositivi.



Nell'immagine su riportata, viene indicato un esempio di come la funzionalità di ZTP possa essere implementata:

- lo switch che deve essere configurato si trova nel Campus 1 che ha il proprio server DHCP.
- L'istanza di AirWave si trova nella sede principale connessa tramite una rete privata.
- Lo switch in modalità factory-default si connette alla rete e invia una richiesta DHCP.

- Il server DHCP nel campus risponde non solo con il pool IP corretto per lo switch, ma anche con le credenziali AirWave, incluso l'indirizzo IP del server AirWave, la cartella, il gruppo e la password condivisa.
- Il processo ZTP dello switch utilizza queste informazioni per comunicare con il server AirWave nella sede centrale.
- Il server AirWave identifica il dispositivo e invia la configurazione associata al gruppo e alla cartella in base a parametri come il numero di modello e l'indirizzo MAC dello switch (se è stato fornito).

MIGLIORA LA PIANIFICAZIONE ED IL PROVISIONING DELLA RETE

- VisualRF consente di eseguire rapidamente pianificazione della copertura RF e cablata per nuovi siti.

GESTISCE LE ULTIME TECNOLOGIE, ARCHITETTURE E PRODOTTI

- Un'unica interfaccia di gestione per più generazioni di dispositivi.
- Supporto di AP autonomi, controllati dal controller e mesh, tra cui Aruba Open AirMesh.
- Monitoraggio di dispositivi wired utilizzando MIB standard.
- Generazione report sull'utilizzo delle porte wired per pianificazione delle capacità.

INTERFACCIA WEB FACILE DA USARE

- Accesso basato sui ruoli, diritti di visualizzazione e amministrazione privilegi su misura per le responsabilità lavorative.
- I grafici personalizzati delle informazioni chiave consentono di eseguire panoramiche e zoom per visibilità in specifici periodi di tempo.
- Identificazione e ricerca utenti per nome.
- Panoramica del cliente riepiloga i tipi di client collegati a la rete e fornisce visibilità ai clienti vegliati o VIP.
- Le visualizzazioni multiple del cruscotto forniscono visibilità su ogni aspetto di RF, client, applicazioni e servizi di rete.

OPZIONI VIRTUALI DELL'APPARECCHIO

La versione virtuale di AirWave è testata per garantire compatibilità e prestazioni con moltissime tipologie di apparati:

- Versione Virtuale che supporta fino a 4.000 dispositivi gestiti.

AirWave richiede una macchina virtuale opportunamente dimensionata

- VMware e Hyper V supportati

Aruba Airwave viene proposto in convenzione come software di gestione on premise, in grado di gestire sia la componente wired, che la componente wireless ed è disponibile in pacchetti di diversi tagli, sulla base del numero di dispositivi che possono essere gestiti dalla piattaforma in maniera centralizzata:

- Software per la gestione fino a 100 nodi (codice prodotto AW-100C)
- Software per la gestione fino a 500 nodi (codice prodotto AW-500C)
- Software per la gestione fino a 1000 nodi (codice prodotto AW-1000C)

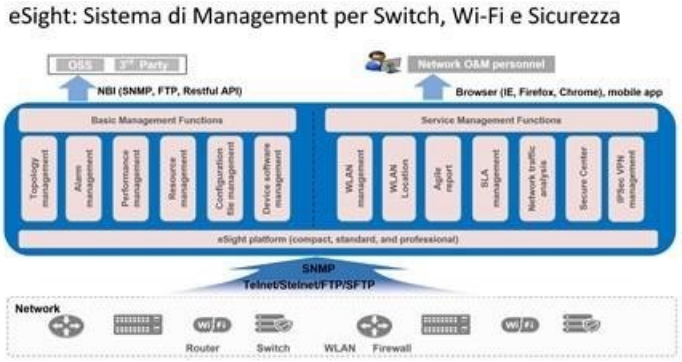
I diversi pacchetti possono essere mixati assieme, anche in tagli differenti e attivati sulla stessa piattaforma centralizzata

HARDWARE

AirWave Enterprise richiede Appliance Enterprise o macchine virtuali (VMware e Hyper-V sono supportati).

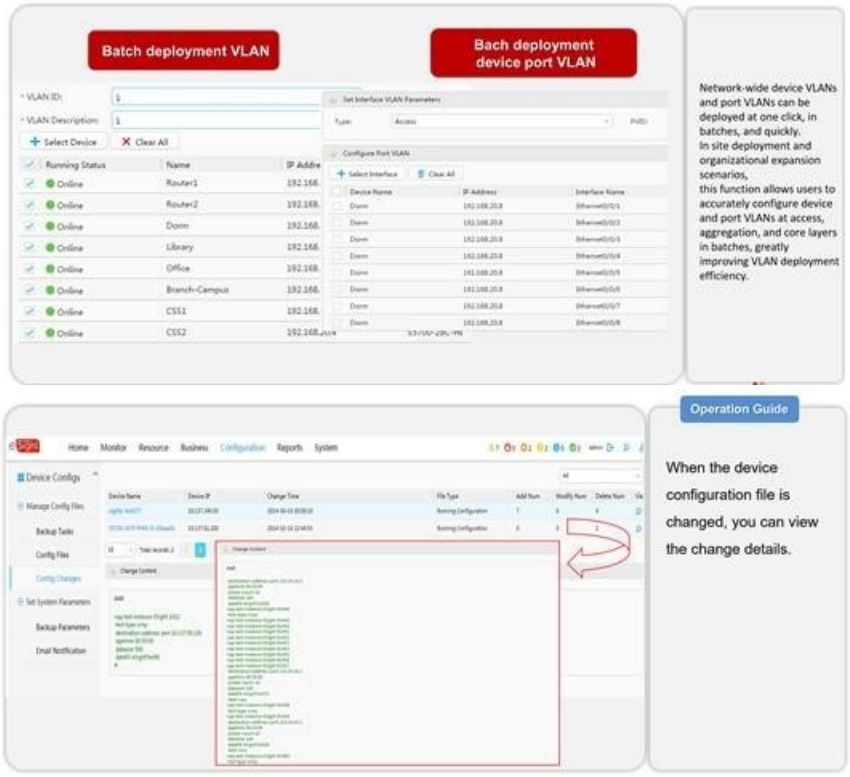
2.10.4. Huawei eSight

eSight è un software avanzato di gestione networking che permette il provisioning, il monitoraggio, allarmistica e ottimizzazione delle prestazioni dell'infrastruttura di rete switching, wireless e next generation firewall. Scala fino a 20000 nodi di rete.



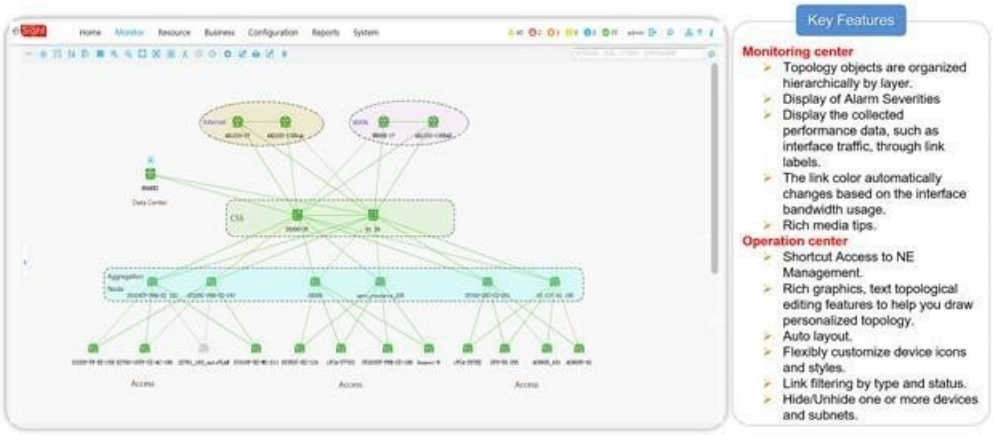
Le interfacce grafiche del software di gestione Wired e Wireless e le tecnologie uniche di visualizzazione dati semplificano la gestione accurata e tempestiva:

- Procedure guidate visive per semplificare le configurazioni e il provisioning dei servizi in maniera più rapida e senza errori;



- Visualizzazioni nt (AP)), corredate con i dati su utilizzo, prestazioni e interferenze, forniscono dettagli immediati sullo stato della rete switched e della Wireless LAN;

- La funzionalità di diagnostica intelligente identifica i guasti nei dispositivi della stazione lato utente (STA) causati da configurazioni sbagliate, ad esempio versioni del sistema operativo, impostazioni dell'adattatore di rete wireless e impostazioni dell'assistenza del sistema sbagliate, rendendo più efficiente la ricerca guasti e riducendo i costi;

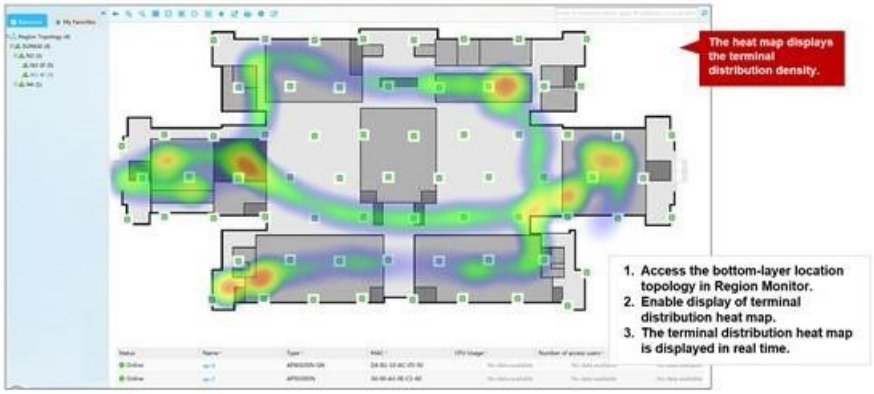


- Vengono utilizzate tecnologie innovative di visualizzazione dei dati, per presentare visualizzazioni il più possibile dettagliate degli access point e degli access controller all'interno della topologia;

- Analisi dello spettro dei segnali di interferenza e rappresentazioni termografiche delle posizioni e della copertura degli access point aiutano l'identificazione dei vuoti e dei conflitti nella copertura;
- Infrastruttura Wired e Wireless LAN costantemente monitorata in tempo reale; visualizzazioni della topologia locale basate sulla logica di rete mostrano access controller, access point, utenti, intensità

di campo della rete wireless e condizioni dei guasti per ogni piano dell'edificio; funzioni per la gestione visiva integrate permettono la risoluzione rapida dei problemi;

- Categorizza, identifica e gestisce client non autorizzati, fonti di interferenza e attacchi di pirateria informatica basandosi sulle regole definite dall'amministratore per ridurre i rischi a cui è sottoposta la rete wireless;
- Wireless Real Location System per la mappatura degli utenti.



2.10.5. ZTE NetNumen U31 R22

Il sistema di management proposto da ZTE è NetNumen U31, è offerto in 3 versioni che differiscono solo per il numero di dispositivi gestiti licenziati.

NetNumen adotta un design modulare, multi-processo e distribuito. È in grado di gestire tutti i prodotti offerti, possiede le funzionalità di gestione, di configurazione, gestione dei fault, manutenzione, sicurezza e reporting.

3. Prodotti per l'accesso Wireless

3.1. Access Point per ambienti interni

3.1.1. Huawei AP4051DN

In fase di sostituzione per End of Sale

3.1.2. ALE AP1201-RWC

Alcatel-Lucent Enterprise OmniAccess Wireless Stellar® AP1201 è un Access-Point WIFI-5, progettato per implementazioni in ambito Enterprise, supporta il protocollo 802.11ac Wave 2, offre un elevato throughput e un'ottima user experience per i client WIFI. L'Access-Point AP1201 supporta un data rate Massimo di 1.2 Gb/s (867 Mb/s in 5 GHz e 400 Mb/s in 2.4 GHz), canali a 80 MHz (VHT80), multi-user MIMO (MU-MIMO) con due spatial streams (2SS) per radio.

Questo Access Point è ideale per l'utilizzo in ambienti di media densità di client WIFI, a titolo di esempio scuole, uffici, ospedali, stazioni, quando un elevato rapporto prestazione-costo è richiesto.

Dotato di tecnologia WLAN con Radio Dynamic Adjustment e di un'architettura Wi-Fi a controllo distribuito, AP1201-RWC consente l'implementazione di rete WFI Enterprise grade e lo rende ideale per i clienti che chiedono una soluzione wireless semplice, sicura e scalabile.

Questo modello in aggiunta integra una radio BLE5.0 / Zigbee a supporto di end-point e applicazioni IoT.

AP1201-RWC può essere implementato in modalità "express mode" attraverso il dispositivo per la gestione AP1221-RWC oppure in modalità "enterprise mode" attraverso il SW di gestione OmniVista 2500 offerto in convenzione come Tipo 10.

Il bundle AP1201-RWC è corredato di supporto per l'installazione a muro o soffitto e di alimentatore AC-DC 48V completo di power-cord con spina italiana per l'alimentazione dello stesso (nel caso non ci sia una alimentazione PoE disponibile).

3.1.3. HPE R0G68AC

La soluzione HPE Aruba che compone la convenzione CONSIP LAN 7 in ambito Wireless è basata sul modello "Instant". La soluzione Aruba Instant prevede che un gruppo di Access Point, in configurazione di default originale, che condividono lo stesso dominio broadcast L2 (la stessa VLAN) sul lato Ethernet, costituiscano automaticamente un cluster coordinato, in cui il primo AP acceso sia il Controller. Le specificità configurative di tutti gli AP del cluster saranno realizzate accedendo il solo controller, che automaticamente le distribuirà sui componenti. Per ogni Controller potrà essere configurato, per esigenze di ridondanza, un backup Controller.

Il limite di scalabilità di un singolo Cluster Instant è di 128 AP. Questo limite in realtà non è dettato dal protocollo di clustering degli AP, ma dalla più generale norma relativa al numero massimo di nodi in un dominio broadcast L2. Pertanto, superato il numero di circa 100 AP, si suggerisce di installare i successivi AP in

una subnet differente a costituire un differente cluster con un nuovo AP Controller. Il modello Instant permette in modo molto semplice ed immediato la realizzazione e la crescita di semplici reti wireless.

Con queste premesse, dunque, analizzando i ruoli dei componenti proposti in convenzione:

Aruba IAP-303P	Access Point per ambienti interni
Aruba Controller 515 - 128 AP Bundle	Dispositivo di Gestione Access Point
Aruba LIC-AW Aruba Airwave with RAPIDS and VisualRF	Software di gestione della piattaforma wireless

Gli AP 303P e 515 sono sia controller che Access point per ambienti interni, in particolare l'AP 515 supporta la tecnologia 802.11ax (WiFi6).

Di seguito vengono riportati i diferenziatori tecnologici e funzionali della soluzione HPE Aruba Instant e relativi Access Point:

Perchè scegliere HPE Aruba

Easy-to-Deploy – semplicità nell'istallazione grazie alla soluzione Instant

Soluzione senza Hardware Controller – La soluzione Instant garantisce un vController distribuito

Altissime prestazioni WiFi e non solo – AP515 unico Access Point / Controller WiFi6 in Convenzione CL7!!! Inoltre, sono dotati di porta Ethernet di tipo SmartRate fino a 2.5Gbps da sfruttare al massimo con Switch di Tipo 5.

Access Point as a Platform – possibilità di interfacciarsi con infrastrutture BLE, ZigBee e Custom Protocol tramite Doogle USB

Alta Affidabilità – ogni AP può assumere il ruolo di controller in caso di fault del Master

Alta Densità – Gli Access Point 515 sono in grado di gestire fino a 512 device simultaneamente

Alta Scalabilità – non limitato a 64 AP bensi 128 AP per ogni Cluster!!!

Risparmio sul Cablaggio – la seconda porta Eth del 303P eroga PoE in uscita per alimentare dispositivi come AP, Telecamere o IoT

Beacon inside – integrato nell'AP Indoor presente in convenzione

Soluzione Aruba Instant abilitante per:

- **Mobile Engagement:** Navigazione indoor degli utenti e push notification
- **Asset Traking:** possibilità controllo e monitoring realtime di strumenti aziendali
- **IoT:** Internet of Things

ClientMatch – ridistribuisce in maniera intelligente i Clients per ogni AP in modo da assicurare le migliori performance al singolo utente. No Sticky Clients!

AppRF – visibilità a 360 gradi delle applicazioni sulla rete Wifi.

Sicurezza – Funzionalità di Firewall L7 integrata nella soluzione Aruba Instant

ARM Adaptive Radio Management – ottimizza il comportamento Wi-Fi e assicura che gli Instant AP stiano alla larga dalle interferenze RF, ottenendo così una rete wireless più affidabile e prestazionale attraverso:

- La selezione automatica del canale e della potenza;
- La rilevazione e riduzione delle interferenze e dei buchi di copertura;
- Il load balancing;

Gestione – Gestione Unificata WiFi–Wired di tutti i prodotti in convenzione Consip Lan 7 grazie al Software Aruba Airwave

Caratteristice Aruba Airwave

- Multivendor
- Zero-touch provisioning
- Tool avanzato per la verifica della copertura ottimale in tempo reale
- Localizzazione Client, Access Point e Access Point non autorizzati (Rogue Access Point) sulle mappe di copertura

Lifetime Warranty – tutti gli AP garantiti a vita con sostituzione NBD

HPE Aruba AP Indoor – AP 303P

VANTAGGI

Gli access point Aruba serie 303 garantiscono la connettività 802.11ac a elevate prestazioni in modo economicamente vantaggioso con MU-MIMO (Wave 2) per ambienti aziendali di media densità.

Con la funzionalità Bluetooth Low Energy (BLE) integrata e il supporto dell'alimentazione 802.3af, gli access point Aruba serie 303 consentono alle aziende di aumentare i livelli di produttività ed efficienza sul lavoro con un TCO ridotto.

I compatti access point Aruba serie 303 offrono la massima velocità dati simultanea, pari a 867 Mb/s nella banda a 5 GHz e a 300 Mb/s nella banda a 2,4 GHz (per una velocità massima aggregata di 1,2 Gb/s). Munito di 2x2:2SS, è stato progettato per ambienti ad alta densità di dispositivi quali scuole, filiali retail, magazzini, strutture alberghiere e uffici aziendali con un ambiente attento ai costi.

I modelli AP-303P supportano il collegamento radio Zigbee 802.15.4 che offre connettività ai dispositivi IoT. Gli access point della serie 300 Wave 2 offrono elevate prestazioni e un'eccezionale esperienza utente per ambienti a media densità.

Gli Access Point indoor sono forniti in modalità bundle e di seguito vengono riportati tutti li accessori inclusi:

Componenti hardware fornite con bundle Aruba AP 303P

- AP R0G68A

- Alimentatore R3K01A
- Cavo di alimentazione JW121A
- Mounting Kit JW047A

Wave 2 802.11ac con 2x2:24SS, 80 MHz e MU-MIMO

- Gli access point Aruba serie 303 supportano le funzionalità 802.11ac con Wave 2, tra cui 2x2:2SS e fino a 80 MHz di larghezza di banda di canale.
- Le radio supportano le trasmissioni in modalità operativa MIMO multiutente (MU-MIMO) e MIMO per utente singolo (SU-MIMO).

Beacon BLE integrato per i servizi di posizione e il monitoraggio degli asset

- Gli access point Aruba serie 303 presentano un beacon Bluetooth Low Energy (BLE) integrato che consente di utilizzare i servizi di localizzazione Aruba, ad esempio la gestione dei beacon, le notifiche di localizzazione e la navigazione.
- L'integrazione del beacon BLE consente alle aziende di sfruttare il contesto della mobilità per lo sviluppo di applicazioni che garantiscono un'esperienza utente migliorata, aumentando in tal modo il valore dell'infrastruttura di rete.

ACC (Advanced Cellular Coexistence)

- Riduce al minimo l'interferenza generata da reti cellulari 3G/4G, sistemi di antenne distribuite e apparecchiature commerciali small cell/femtocell.

QoS per la visibilità e il controllo delle app

- Supporta la gestione delle priorità e l'applicazione delle policy per app di comunicazioni unificate, tra cui Microsoft Skype for Business con dati crittografati di videoconferenze, voce, chat e condivisione di desktop

Gestione RF

- La tecnologia Adaptive Radio Management (ARM) assegna automaticamente le impostazioni di canale e di potenza trasmissiva, fornisce airtime fairness e fa sì che gli AP operino senza fonti di interferenza RF per garantire WLAN affidabili e ad alte prestazioni
- Gli AP della serie 300 di Aruba possono essere configurati per fornire funzionalità di air monitoring part-time o dedicato per analisi dello spettro e protezione dalle intrusioni wireless, tunnel VPN per estendere le sedi remote alle risorse aziendali e connessioni wireless mesh dove non siano disponibili cavi Ethernet.

Visibilità e controllo intelligenti delle applicazioni

- La tecnologia AppRF si serve dell'esame approfondito dei pacchetti per classificare e bloccare, dare priorità o limitare la larghezza di banda per oltre 2.500 app aziendali o gruppi di app.

Sicurezza

- La protezione dalle intrusioni wireless integrata protegge dalle minacce e le riduce, eliminando al contempo l'esigenza di sensori RF e applicazioni di sicurezza separate
- I servizi per la reputazione e la sicurezza dell'IP identificano, classificano e bloccano i file, gli URL e gli IP malevoli, fornendo una protezione avanzata dalle minacce online
- Tecnologia TPM (Integrated Trusted Platform Module) per l'archiviazione sicura di credenziali e chiavi

Monitoraggio intelligente dell'alimentazione (IPM)

- Consente all'AP di monitorare costantemente e segnalare il consumo energetico effettivo e, facoltativamente, di prendere decisioni autonome per disattivare determinate funzionalità
- Negli AP della serie 300, la funzionalità IPM per il risparmio energetico si applica quando l'unità è alimentata da una fonte 802.3af PoE. Per impostazione predefinita, l'interfaccia USB sarà la prima caratteristica a disattivarsi se il consumo energetico dell'AP supera il budget disponibile. In rare occasioni può essere necessario adottare ulteriori misure per il risparmio energetico, ma nella maggior parte dei casi gli AP della serie 300 operano in modalità illimitata

Ampia scelta delle modalità operative

- Gli AP della serie 300 di Aruba offrono una serie di modalità operative per soddisfare requisiti di gestione e installazione specifici.
- Modalità gestita da controller: quando sono gestiti tramite Mobility Controller di Aruba, gli AP Aruba della serie 300 offrono funzionalità di configurazione centralizzata, crittografia dei dati, applicazione delle politiche e servizi di rete, nonché inoltro distribuito e centralizzato del traffico
- Modalità Aruba Instant: in modalità Aruba Instant, un singolo AP distribuisce automaticamente la configurazione di rete agli altri AP Instant nella WLAN. Basta accendere un Instant AP, configurarlo via Wi-Fi e collegare gli altri AP: l'intera procedura richiede circa cinque minuti. Se i requisiti della WLAN cambiano, un percorso di migrazione integrato consente agli AP Instant della serie 300 di divenire parte di una WLAN gestita da un Mobility Controller
- AP remoto (RAP) per l'implementazione nelle filiali
- AM (Air Monitor) per IDS wireless, rilevamento e contenimento di server non autorizzati
- Analizzatore dello spettro, dedicato o ibrido, per l'identificazione delle fonti di interferenza RF
- Mesh aziendale sicura
- Per le installazioni di grandi dimensioni su più siti, il servizio Aruba Activate riduce notevolmente i tempi di installazione automatizzando il provisioning dei dispositivi, gli upgrade del firmware e la gestione dell'inventario. Con Aruba Activate, gli Instant AP sono spediti dallo stabilimento a qualsiasi sede e si configurano autonomamente all’accensione.

Specifiche

Radio 802.11ac - 5 GHz 2x2 MIMO (867 Mbps di velocità massima) e 2,4 GHz 2x2 MIMO (300 Mbps di velocità massima) con antenne integrate.

Specifiche radio wi-fi

- Tipo di AP: da uso interno, dual radio, 5GHz 802.11ac 2x2 MIMO e 2,4-GHz 802.11n 2x2 MIMO.
- Dual radio configurabile tramite software, supporta 5 GHz (Radio 0) e 2,4 GHz (Radio 1)
- 5GHz: Single User (SU) MIMO con 2 flussi spaziali per una velocità dati wireless massima di 867 Mbps a dispositivi client singoli 2x2 VHT80
- 5GHz: Multi User (MU) MIMO con due flussi spaziali per una velocità dati wireless massima di 867 Mbps fino a due (1x1 VHT80) dispositivi client MU-MIMO contemporaneamente
- 2,4GHz: Single User (SU) MIMO con due flussi spaziali per una velocità dati wireless massima di 300 Mbps a dispositivi client singoli 2x2 HT40 (300 Mbps per dispositivi client HT40 802.11n)
- Supporto di un massimo di 256 dispositivi client associati per radio e di massimo 16 BSSID per radio
- Bande di frequenze supportate (si applicano restrizioni specifiche di singoli paesi):
- Da 2,400 a 2,4835 GHz
- Da 5,150 a 5,250 GHz
- Da 5,250 a 5,350 GHz
- Da 5,470 a 5,725 GHz
- Da 5,725 a 5,850 GHz
- Canali disponibili: a seconda del dominio regolatore configurato
- La selezione dinamica delle frequenze (DFS, Dynamic Frequency Selection) ottimizza l'utilizzo dello spettro RF disponibile
- Tecnologie radio supportate:
- 802.11b: DSSS (Direct-Sequence Spread-Spectrum)
- 802.11a/g/n/ac: OFDM (Orthogonal Frequency-Division Multiplexing)

Tipi di modulazione supportati:

- 802.11b: BPSK, QPSK, CCK
- 802.11a/g/n/ac: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM
- Potenza di trasmissione: configurabile in incrementi di 0,5 dBm
- Potenza di trasmissione massima (condotta), limitata da requisiti normativi locali:
- Banda 2,4 GHz: +18 dBm per chain, +21 dBm aggregata (2x2)
- Banda 5GHz: +18 dBm per chain, +23 dBm aggregata (3x3)
- La funzionalità ACC (Advanced Cellular Coexistence) riduce al minimo l'interferenza generata dalle reti cellulari
- Tecnologia MRC (Maximum Ratio Combining) per prestazioni del ricevitore ottimizzate
- Tecnologia CDD/CSD (Cyclic Delay/Shift Diversity) per prestazioni RF in downlink ottimizzate
- Intervallo di guardia breve per i canali a 20 MHz, 40 MHz, 80MHz e 80 MHz
- Codifica STBC (Space-Time Block Coding) per un maggiore intervallo e una ricezione ottimizzata
- Tecnologia LDPC (Low-Density Parity Check) per una correzione degli errori ad alta efficienza e un throughput più elevato
- Beamforming di trasmissione (TxBF) per una migliore affidabilità e raggio del segnale

Velocità dei dati supportate (Mbps):

- 802.11b: 1, 2, 5,5, 11
- 802.11a/g: 6, 9, 12, 18, 24, 36, 48, 54
- 802.11n: da 6,5 a 300 (da MCS0 a MCS15)

- 802.11ac: da 6,5 a 867 (da MCS0 a MCS9, NSS = da 1 a 2)
- Supporto 802.11n High-Throughput (HT): HT 20/40
- Supporto 802.11ac VHT: VHT 20/40/80
- Aggregazione pacchetti 802.11n/ac: A-MPDU, A-MSDU

Antenne wi-fi

- Due antenne omnidirezionali dual-band polarizzate verticalmente per 2x2 MIMO, con picco di guadagno di antenna 3.4dBi in 2.4GHz e 7.8dBi in 5GHz.
- Le antenne sono ottimizzate per il montaggio orizzontale a soffitto dell'AP.

Altre interfacce

- Una interfaccia di rete 10/100/1000BASE-T Ethernet (RJ-45)
- rilevamento automatico della velocità di collegamento e MDI/MDX
- 802.3az EEE (Energy Efficient Ethernet)
- PoE-PD: 48Vdc (nominale) 802.3af PoE
- Una interfaccia di rete 10/100/1000BASE-T Ethernet (RJ-45)
- Rilevamento automatico della velocità di collegamento e MDI/MDX
- 802.3az EEE (Energy Efficient Ethernet)
- PSE (output): 48Vdc (nominale) 802.3af/at PoE

Alimentazione dei Dispositivi in cascata al 303P

- Radio BLE (Bluetooth Low Energy)
- Radio Zigbee 802.15.4
- Indicatori visivi (LED multicolore): per lo stato di sistema e della radio
- pulsante di reset: reset alle impostazioni di fabbrica (durante l'avviamento del dispositivo)
- Interfaccia per porta console seriale (proprietaria; disponibile cavo adattatore opzionale)
- Slot di sicurezza Kensington

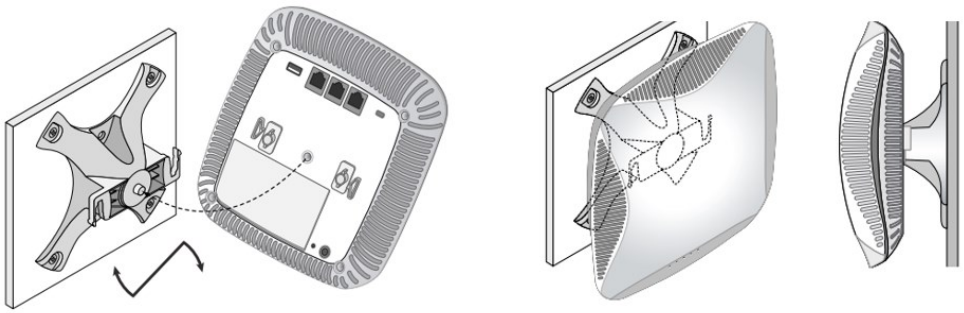
Sorgenti di alimentazione e consumo

- L'AP supporta l'alimentazione DC diretta e Power over Ethernet (PoE)
- Quando sono disponibili entrambe le sorgenti di alimentazione, l'alimentazione DC ha la priorità sul PoE
- Gli alimentatori sono venduti separatamente
- Sorgente DC diretta: 58Vdc nominali, +/- 5%
- L'interfaccia accetta una spina circolare con positivo centrale da 1,35/3,5 mm con lunghezza di 9,5 mm
- Power over Ethernet (PoE) per le porte Ethernet0: sorgente conforme a 802.3af/802.3at a 48 Vdc (nominali)
- La funzionalità di PoE-PSE è disabilitata sull'interfaccia Ethernet1 quando alimentato da sorgente PoE 802.3af
- Massimo consumo di energia: 11,3W (PoE) o 11,5W (DC)
- Massimo consumo di energia in modalità inattiva: 6,8W (PoE) o 7W (DC)
- I consumi riportati non comprendono il caso di alimentazione PoE-PSE su porta Ethernet1

Montaggio

L'AP viene fornito in dotazione clip di montaggio (colore bianco) per il montaggio a parete / soffitto su superficie piana (base, superficie piana).

- Mount kit fornito nel Bundle di convenzione:
  - AP-220-MNT-W1W



HPE Aruba AP-220-MNT-W1W

Caratteristiche fisiche

- Dimensioni/peso dell'unità esclusi gli accessori di montaggio:
- 150mm x 150mm x 35mm
- 280g
- Dimensioni/peso (confezione di spedizione):
- 190mm x 180mm x 60mm
- 430g

Condizioni ambientali

- Funzionamento:
- Temperatura: da 0°C a +40°C
- Umidità: da 5% a 93% senza condensa
- Immagazzinaggio e trasporto:
- Temperatura: da -40°C a +70°C

Conformità normativa

- FCC/ISED
- Marchio CE
- Direttiva RED 2014/53/EU
- Direttiva EMC 2014/30/EU
- Direttiva 2014/35/EU sulla bassa tensione
- UL/IEC/EN 60950
- EN 60601-1-1 e EN 60601-1-2

Affidabilità

- Tempo medio fra i guasti (MTBF): 518000 ore (59 anni) a una temperatura di esercizio di +25 gradi

Certificazioni

- CB Scheme Safety, cTUVus
- UL2043 Plenum Rating
- Certificato Wi-Fi Alliance (WFA) 802.11a/b/g/n/ac
- WPA, WPA2 and WPA3 – Enterprise with CNSA option, Personal (SAE), Enhanced Open (OWE)
- Wi-Fi Alliance certified (WFA) 802.11ac with Wave 2 features
- Passpoint® (Release 2) con ArubaOS e Instant 8.3+

Garanzia

- Garanzia a vita limitata Aruba

Versioni minime del software

- ArubaOS 8.4.0.0
- Aruba InstantOS 8.4.0.0

Per maggiori Informazioni e per una documentazione esaustiva in merito ai prodotti e la guida utile alla configurazione, si rimanda al seguente link: Aruba Network Architecture WiFi

3.2. Access Point per ambienti esterni

3.2.1. Huawei AP8150DN

In fase di sostituzione per End of Sale

3.2.2. ALE AP1251-RWC

Alcatel-Lucent Enterprise OmniAccess Wireless Stellar® AP1251 è un Access-Point WIFI-5, ad alte prestazioni utilizzato in ambienti esterni per implementazioni in ambito Enterprise, supporta il protocollo 802.11ac Wave 2 offre un elevato throughput e un'ottima user experience. L'Access-Point AP1251 da esterno supporta un data rate Massimo di 867 Mb/s a 5 GHz e 400 Mb/s a 2,4 Ghz, canali a 80 MHz (VHT80), multi-user MIMO (MU-MIMO) con due spatial streams (2SS) per radio. L'AP1251 è un dispositivo robusto che supporta lo standard IP67 per l'utilizzo in ambienti difficili.

Questo Access Point è ideale per l'utilizzo all'esterno o in ambienti industriali critici, per estendere la copertura WIFI e di conseguenza la mobilità per i client in aree prive di protezioni alle temperature e agli agenti atmosferici, a titolo di esempio aree outdoor di campus universitari, ospedali, parchi pubblici, piazze e stazioni.

Dotato di tecnologia WLAN con Radio Dynamic Adjustment e di un'architettura Wi-Fi a controllo distribuito, AP1251-RWC consente l'implementazione di rete WFI Enterprise grade e lo rende ideale per i clienti che chiedono una soluzione wireless semplice, sicura e scalabile.

Questo modello fornisce una porta di downlink 1Gbps per il collegamento di end-point IoT.

AP1251-RWC può essere implementato in modalità "express mode" mediante il dispositivo per la gestione AP1221-RWC oppure in modalità "enterprise mode" attraverso il SW di gestione OmniVista 2500 offerto in convenzione come Tipo 10.

Il bundle AP1251-RWC è corredato di staffe per l'installazione su palo o a muro e di alimentatore Power Injector completo di power-cord con spina italiana per l'alimentazione dello stesso (nel caso non ci sia una alimentazione PoE disponibile).

3.2.3. HPE JZ162AC

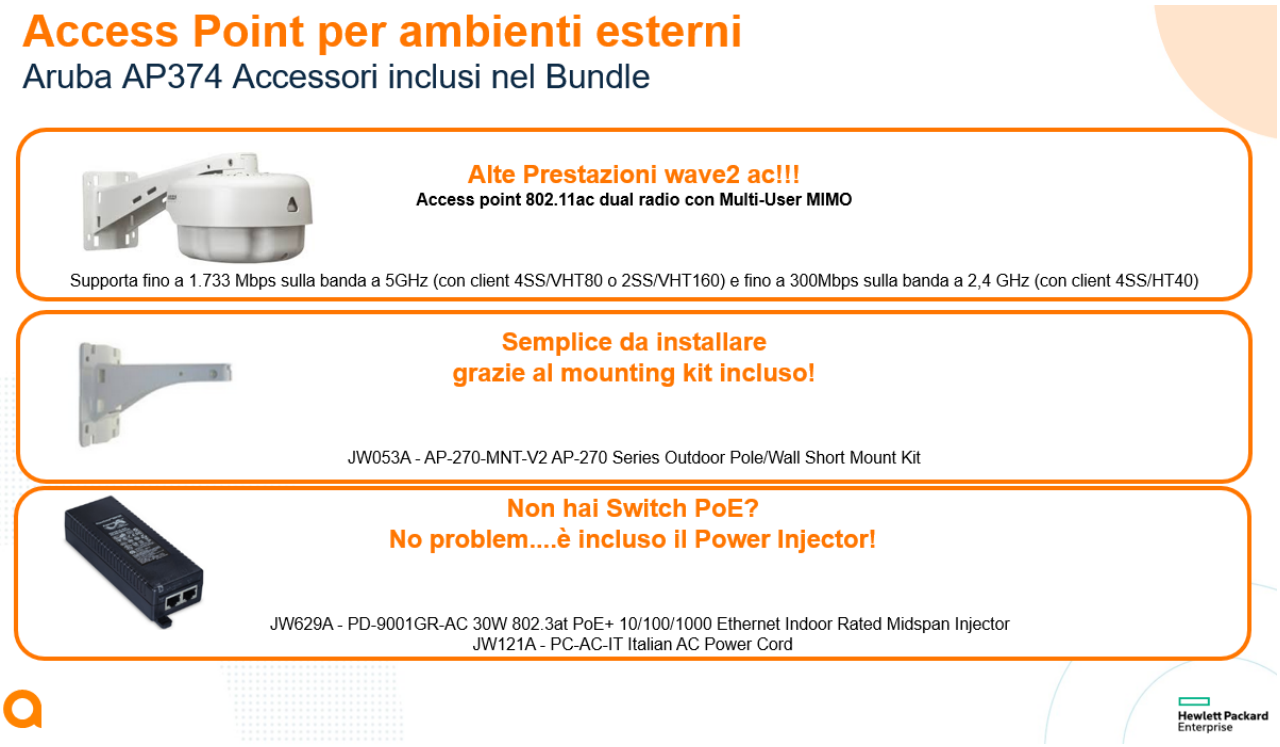
HPE Aruba AP 374

VANTAGGI

A prova di intemperie e resistenti agli sbalzi di temperatura, gli access point Aruba serie 370 offrono lo standard 802.11ac Wave 2 espressamente concepito per esterni e ubicazioni difficili dal punto di vista ambientale. La serie Aruba 370 con potenza e prestazioni elevate offre maggiori capacità e raggio d'azione. Offre capacità 4x4:4SS MU-MIMO, oltre al ClientMatch avanzato di Aruba e un beacon Bluetooth integrato per abilitare i

servizi di localizzazione Aruba. Espressamente concepiti per gli ambienti esterni più ostili, gli access point serie 370 sono in grado di sopportare temperature estreme, oltre a precipitazioni e umidità persistenti, e sono completamente sigillati per impedire l'ingresso dei contaminanti aerei. Tutte le interfacce elettriche sono dotate di protezione dalle sovratensioni di livello industriale. I dispositivi della serie Aruba 370 sono inoltre dotati di beacon Bluetooth Aruba integrato, che semplifica la gestione remota di una rete su vasta scala di beacon Aruba alimentati a batteria, fornendo al tempo stesso avanzate funzioni di localizzazione e ricerca di percorsi, oltre a servizi di notifica push e monitoraggio degli asset.

Gli Access Point outdoor sono forniti in modalità bundle e di seguito vengono riportati tutti li accessori inclusi:



Componenti hardware fornite con bundle Aruba AP 374

- AP JZ162A
- Power Injector JW629A
- Cavo di alimentazione JW121A
- Mounting Kit JW053A
- N. 6 Antenne Dual-Band Omnidirezionali

Access point 802.11ac dual radio con Multi-User MIMO

- Supporta fino a 1.733 Mbps sulla banda a 5GHz (con client 4SS/VHT80 o 2SS/VHT160) e fino a 300Mbps sulla banda a 2,4 GHz (con client 4SS/HT40)

Radio Bluetooth Low-Energy (BLE) integrata

- Abilita i servizi di localizzazione con i dispositivi mobili compatibili con BLE che ricevono segnali da più Aruba Beacon contemporaneamente.

ACC (Advanced Cellular Coexistence)

- Riduce al minimo l'interferenza generata da reti cellulari 3G/4G, sistemi di antenne distribuite e apparecchiature commerciali small cell/femtocell.

Design industriale per ambienti indoor e outdoor ostili

- Interfacce di connessione sigillate per impedire infiltrazioni di polvere e umidità

QoS per applicazioni di comunicazioni unificate

- Supporta la gestione delle priorità e l'applicazione delle politiche per app di comunicazioni unificate, tra cui Microsoft Skype for Business con dati crittografati di videoconferenze, voce, chat e condivisione di desktop.

Gestione RF avanzata

- La tecnologia AirMatch integrata gestisce le bande radio 2,4 GHz e 5 GHz e ottimizza attivamente l'ambiente RF, inclusa l'ampiezza del canale, la selezione dei canali e la potenza di trasmissione.

Analisi di spettro

- In grado di eseguire funzioni di air monitoring part-time o dedicato, l'analizzatore di spettro esegue in modalità remota la scansione delle bande radio a 2,4 GHz e 5 GHz per individuare le sorgenti di interferenze RF.

Wireless mesh

- Le connessioni wireless mesh risultano comode dove non sono disponibili cavi Ethernet.

Visibilità e controllo intelligenti delle applicazioni

- AppRF sfrutta tecnologia deep packet inspection per classificare, bloccare, limitare la larghezza di banda o definirne le priorità per migliaia di app aziendali o gruppi di app.

Aruba Secure Core

- Garanzia dispositivo: uso di Trusted Platform Module (TPM) per l'archiviazione sicura delle credenziali e delle chiavi, oltre all'avvio sicuro.
- La protezione dalle intrusioni wireless integrata protegge dalle minacce e le riduce, eliminando al contempo l'esigenza di sensori RF e applicazioni di sicurezza separate.
- I servizi per la reputazione e la sicurezza IP identificano, classificano e bloccano i file, gli URL e gli IP malevoli, fornendo una protezione avanzata dalle minacce online.
- I tunnel VPN IPsec crittografati collegano in remoto gli utenti alle risorse di rete aziendali.

Modalità operativa a scelta

In quanto AP unificato, Aruba 370 può essere implementato con o senza controller e prontamente commutato per l'adeguamento alle nuove esigenze di rete:

- Modalità controller: se gestiti tramite Mobility Controller Aruba, gli AP serie 370 offrono configurazione centralizzata, crittografia dei dati, applicazione delle politiche e servizi di rete, oltre all'inoltro distribuito e centralizzato del traffico.
- Modalità senza controller (Instant): nella modalità Aruba Instant, un singolo AP distribuisce automaticamente la configurazione di rete ad altri AP in modalità Instant nella WLAN. Sarà sufficiente accendere un AP in modalità Instant, configurarlo via Wi-Fi e collegare gli altri AP (Instant Network).

Altre modalità funzionali includono:

- Modalità Remote AP (RAP) per le implementazioni a livello di filiale
- AM (Air Monitor) per IDS wireless, rilevamento e contenimento di access point rogue non autorizzati
- Analizzatore dello spettro, dedicato o ibrido, per l'identificazione delle fonti di interferenza RF
- Mesh aziendale sicura
- L'AP ibrido serve i client Wi-Fi e fornisce protezione dalle intrusioni wireless e analisi di spettro

Per le installazioni di grandi dimensioni su più siti, il servizio Aruba Activate riduce notevolmente i tempi di implementazione automatizzando il provisioning dei dispositivi, gli upgrade del firmware e la gestione dell'inventario. Con Aruba Activate, gli AP unificati vengono spediti dallo stabilimento a qualsiasi sede e all'accensione verranno configurati automaticamente.

Specifiche

- 5 GHz 802.11ac 4x4 MU-MIMO (velocità massima pari a 1.733 Mbps)
    - Quattro connettori Nf per antenne esterne
- Radio 2,4 GHz 802.11n 2x2 MIMO (velocità massima 300 Mbps)
    - Due connettori Nf per antenne esterne 2,4 GHz

Specifiche radio wi-fi

- Tipo di AP: uso outdoor a protezione avanzata, dual radio, 5 GHz 802.11ac 4x4 MIMO e 2,4 GHz 802.11n 2x2 MIMO
- Dual radio configurabile tramite software, supporta 5 GHz (Radio 0) e 2,4 GHz (Radio 1);
    - 5 GHz:
        - Multi User (MU) MIMO con quattro flussi spaziali per una velocità dati wireless massima di 1.733 Mbps fino a tre dispositivi client MU-MIMO contemporaneamente
        - Single User (SU) MIMO con quattro flussi spaziali per una velocità dati wireless massima di 1.733 Mbps a dispositivi client singoli 4x4 VHT80 o 2x2 VHT160
    - 2,4 GHz:

        - Single User (SU) MIMO con due flussi spaziali per una velocità dati wireless massima di 300 Mbps a dispositivi client singoli 2x2 HT40
- Supporto di un massimo di 256 dispositivi client associati per radio e di massimo 16 BSSID per radio
- Bande di frequenza supportate (si applicano restrizioni specifiche di singoli Paesi):
    - Da 2,400 a 2,4835 GHz
    - Da 5,150 a 5,250 GHz
    - Da 5,250 a 5,350 GHz
    - Da 5,470 a 5,725 GHz
    - Da 5,725 a 5,850 GHz
- Canali disponibili: a seconda del dominio regolatore configurato.
- La selezione dinamica delle frequenze (DFS, Dynamic Frequency Selection) ottimizza l'uso dello spettro RF disponibile.
- Tecnologie radio supportate:
    - 802.11b: DSSS (Direct-Sequence Spread-Spectrum)
    - 802.11a/g/n/ac: OFDM (Orthogonal Frequency-Division Multiplexing)
- Tipi di modulazione supportati:
    - 802.11b: BPSK, QPSK, CCK
    - 802.11a/g/n/ac: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM
- Potenza di trasmissione: configurabile in incrementi di 0,5 dBm
- Potenza di trasmissione massima (condotta), limitata da requisiti normativi locali:
    - Banda 2,4 GHz: +22 dBm per chain, +25dBm aggregata (2x2)
    - Banda 5 GHz: +22 dBm per chain, +28dBm aggregata (4x4)
    - Nota: i livelli di potenza di trasmissione condotta escludono il guadagno dell'antenna.
- EIRP massimo (con limitazioni imposte dai requisiti normativi locali):
    - Banda 2,4 GHz:
        - 375: EIRP 29 dBm
    - Banda 5 GHz:
        - 374: 28 + guadagno antenna + guadagno TxBF
- La funzionalità ACC (Advanced Cellular Coexistence) riduce al minimo l'interferenza generata dalle reti cellulari.
- Tecnologia MRC (Maximum Ratio Combining) per prestazioni del ricevitore ottimizzate.
- Tecnologia CDD/CSD (Cyclic Delay/Shift Diversity) per prestazioni RF in downlink ottimizzate.
- Short guard interval per i canali 20 MHz, 40 MHz, 80 MHz e 160 MHz.
- Codifica STBC (Space-Time Block Coding) per una maggiore copertura e una ricezione ottimizzata.
- Tecnologia LDPC (Low-Density Parity Check) per una correzione degli errori ad alta efficienza e un throughput più elevato.
- Beamforming di trasmissione (TxBF) per una migliore affidabilità e raggio del segnale.
- Velocità dei dati supportate (Mbps):
    - 802.11b: 1, 2, 5,5, 11
    - 802.11a/g: 6, 9, 12, 18, 24, 36, 48, 54
    - 802.11n (2,4GHz): da 6,5 a 300 (da MCS0 a MCS15)
    - 802.11n (5GHz): da 6,5 a 600 (da MCS0 a MCS31)
    - 802.11ac: da 6,5 a 1.733 (da MCS0 a MCS9, NSS = da 1 a 4 per VHT20/40/80, NSS = da 1 a 2 per VHT160)

- Supporto 802.11n High-Throughput (HT): HT 20/40
- Supporto VHT (very high throughput) 802.11ac: VHT 20/40/80/160
- Aggregazione pacchetti 802.11n/ac: A-MPDU, A-MSDU

Alimentazione

- Consumo massimo di energia dell'AP: 23W
- Alimentatori venduti separatamente
- Power over Ethernet (PoE+): conforme a 802.3at
- Alimentazione AC: AC 100-240 volt 50/60 Hz

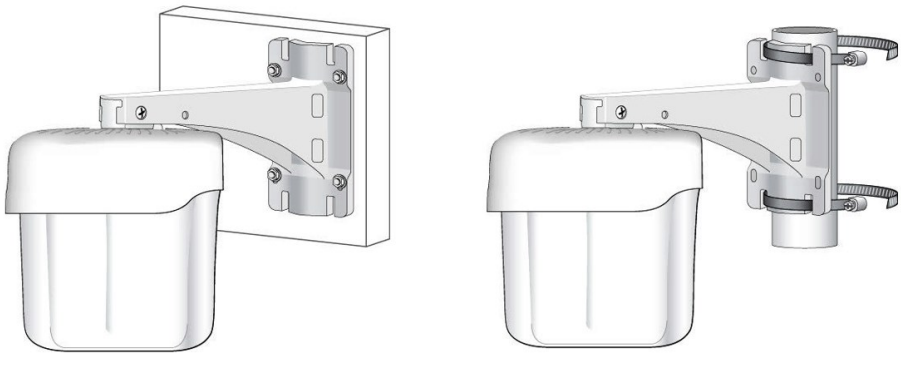
Altre interfacce

- Interfacce di rete 10/100/1000BASE-T Ethernet (RJ-45):
  - Rilevamento automatico della velocità di collegamento e MDI/MDX
  - 802.3az EEE (Energy Efficient Ethernet)
- Una porta SFP 1000BASE-X
- Radio BLE (Bluetooth Low Energy):
  - Fino a 4 dBm di potenza di trasmissione (classe 2) e -91 dBm di sensibilità di ricezione
- Indicatore visivo (LED multicolori): per stato di sistema e radio
- Pulsante di reset: reset alle impostazioni di fabbrica (durante l'avviamento del dispositivo)
- Interfaccia console micro-USB
- Slot di sicurezza Kensington

Montaggio

L'AP viene fornito in dotazione con staffa di montaggio su asta / parete verticale (colore bianco)

- Mount kit fornito nel Bundle di convenzione:
  - AP-270-MNT-V2

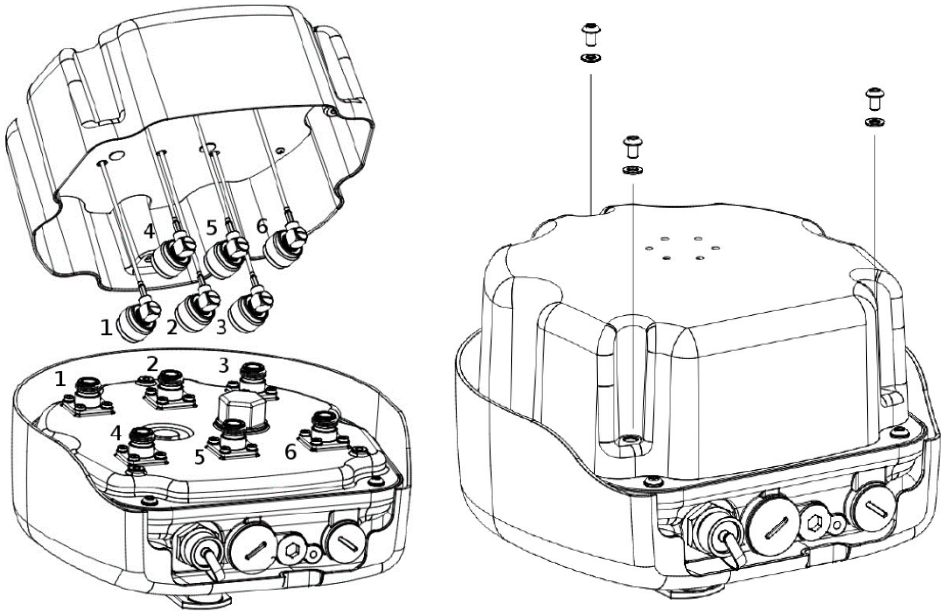


HPE Aruba AP-270-MNT-V2

Antenne

L'AP viene fornito in dotazione con N. 6 Antenne Dual-Band Omnidirezionali modello TW-6X AR374:

- ANTENNA MIMO 4X4 5GHZ + 2X2 2,4GHZ



Caratteristiche fisiche

- Dimensioni/peso con cover estetica (montaggio escluso):
  - 23 cm (L) x 24 cm (P) x 19 cm (A)
  - 9,0" (L) x 9,4" (P) x 7,5" (A)
  - 2,7 kg/6 lbs
- Dimensioni/peso senza cover estetica (montaggio escluso):
  - 23 cm (L) x 24 cm (P) x 14 cm (A)
  - 9,0" (L) x 9,4" (P) x 5,5" (A)
  - 2,4 kg/5,3 lbs

Condizioni ambientali

- Funzionamento:
  - Temperatura: da -40 °C a +65 °C
  - Umidità: da 5% a 95% senza condensa
- Immagazzinaggio e trasporto:
  - Temperatura: da 40°C a +70°C
- Altitudine di funzionamento:
  - 3.000 metri
- Acqua e polvere
  - IP66/67
- Tolleranza al sale
  - Testato secondo ASTM B117-07A Spray sale 200 ore
- Resistenza al vento: fino a 165 mph
  - Urti e vibrazioni: ETSI 300-19-2-4

Conformità normativa

- FCC/ISED
- Marchio CE
- Direttiva RED 2014/53/EU
- Direttiva EMC 2014/30/UE
- Direttiva sulla bassa tensione 2014/35/UE
- UL/IEC/EN 60950
- EN 60601-1-1, EN60601-1-2

Per ulteriori informazioni e approvazioni normative specifiche dei singoli Paesi, rivolgersi al proprio rappresentante Aruba.

Numeri di modello normativo

- AP-374: APEX0374

Certificazioni

- CB Scheme Safety, cTUVus
- UL2043 Plenum Rating
- Certificato Wi-Fi Alliance 802.11a/b/g/n
- Wi-Fi CERTIFIED™ ac (con funzionalità Wave 2)

Garanzia

- Garanzia limitata a vita Aruba

Versioni minime del software

- ArubaOS e Aruba InstantOS 8.3.0.0

Per maggiori Informazioni e per una documentazione esaustiva in merito ai prodotti e la guida utile alla configurazione, si rimanda al seguente link: Aruba Network Architecture WiFi.

3.3. Dispositivo di gestione degli Access Point

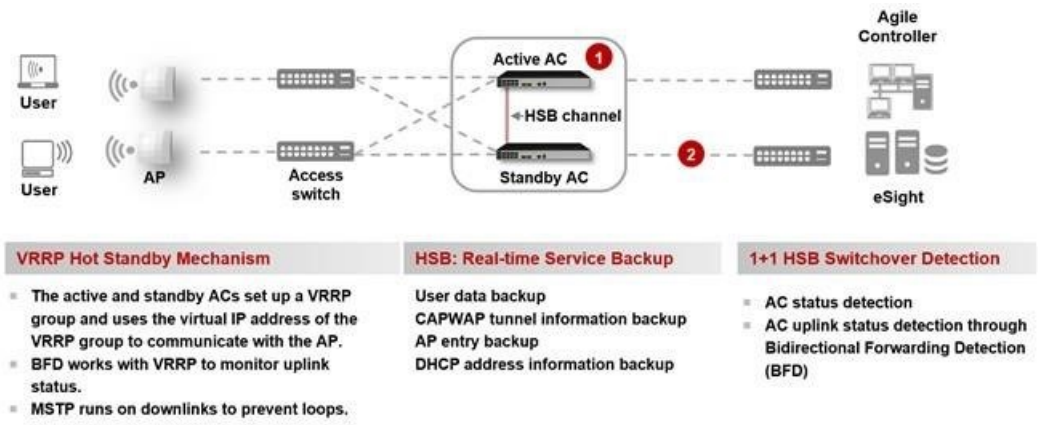
3.3.1. Huawei AC6508

L'access controller Huawei AC6508 permette servizi di accesso via cavo o wireless nelle reti aziendali per complessi edilizi, uffici, filiali di piccole e medie imprese. L'architettura Fit AP + AC flessibile e robusta permette un inoltro a 6 Gbit/s, gestisce 256 AP e supporta fino a 64000 accessi utente ed è facilmente scalabile se occorre. Il modello AC6508 ha 10 porte 1GE + 6 porte 10GE Combo rame o ottiche SFP+.

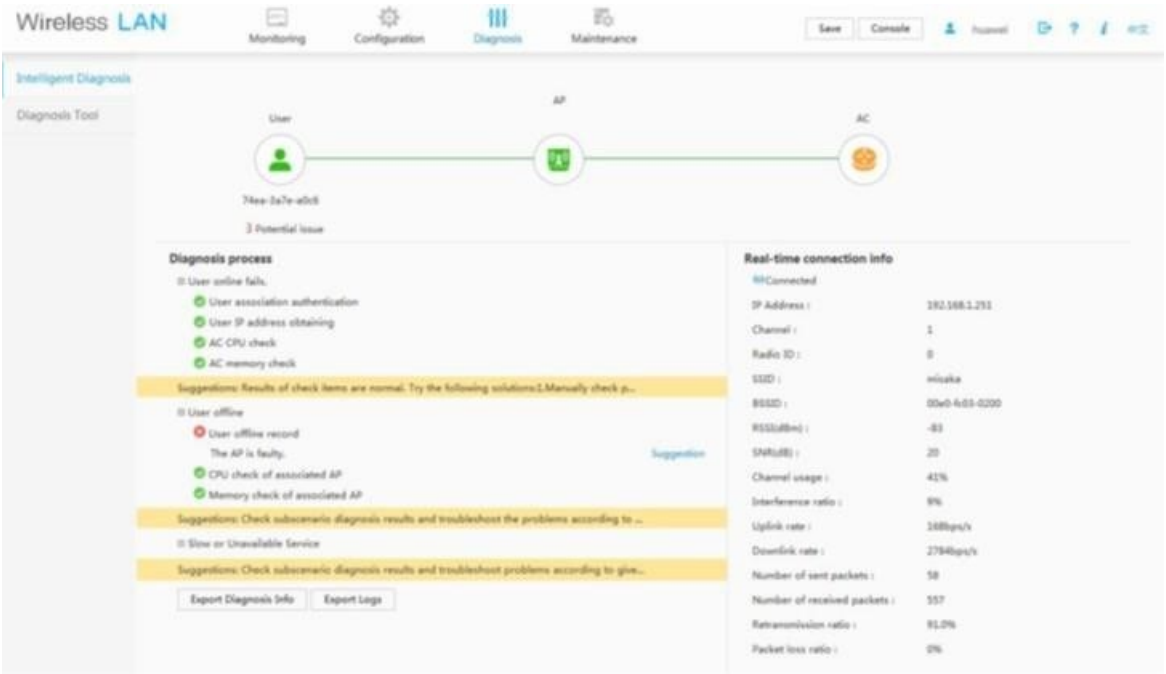
Permette flessibilità nell'inoltro dati: diretto (local forwarding) o via tunneling (central forwarding) e una gestione flessibile e dettagliata dei diritti degli utenti con un controllo accesso basato su utenti e ruoli, importazione e sincronizzazione via servizi di directory esterna, politiche di sicurezza e QoS su base applicativa (Traffic Identification) sul traffico utente.

Supporta gli scenari di alta affidabilità (clustering di 2 Controller) in maniera da garantire continuità di servizio e convergenza sotto i 50 ms dopo un malfunzionamento.

È fornito in Convenzione licenziato per gestire fino a 64 AP. Configurati in alta affidabilità, le licenze si condividono, quindi 2 x Wi-Fi Controller configurati da Convenzione supportano 128 Access Point senza ulteriori licenze da aggiungere.



La gestione energetica dinamica riduce i consumi totali; aumenta le prestazioni e riduce ulteriormente i consumi energetici se accoppiato con un sistema di gestione intelligente come eSight NMS.



È gestibile (configurazione, monitoraggio e allarmistica) dal sistema di management eSight (Tipo 10) incluso all'interno della Convenzione.

3.3.2. ALE AP1221-RWC

Alcatel-Lucent Enterprise OmniAccess Wireless Stellar® AP1221 è un Access-Point WIFI-5 di fascia medio-alta che utilizza protocollo 802.11ac Wave 2, ideale per l'utilizzo in soluzioni che richiedono un alta densità di client grazie ad un data rate di 2.1 Gb/s (1733 Mb/s in 5 GHz e 400 Mb/s in 2.4 GHz), canali a 160 MHz (VHT160), multi-user MIMO (MU-MIMO) con 4 spatial streams (4SS) a 5Ghz e 2 spatial stream (2SS) a 2,4Ghz.

AP1221 è utilizzato per la gestione di cluster di Access Point indoor o outdoor fino a 64 elementi, fornendo il management plane centralizzato e contestualmente l'erogazione di funzionalità WIFI verso i client.

In base all'esigenza è possibile introdurre più AP1220 nella configurazione al fine di fornire alta affidabilità alla funzione di gestione del cluster.

Con questo dispositivo, è possibile indirizzare le richieste di capitolato sfruttando la modalità implementativa denominata "express mode", che consente di gestire gli Access-Pont della famiglia Stellar offerti in convenzione attraverso la funzione di management integrata nel sistema operativo.

AP1221-RWC può anche essere implementato come Access Point in modalità "enterprise mode" mediante il SW di gestione OmniVista 2500 offerto in convenzione come Tipo 10.

Il bundle AP1221-RWC è corredato di supporto per l'installazione a muro o soffitto e di alimentatore AC-DC 48V completo di power-cord con spina italiana per l'alimentazione dello stesso (nel caso non ci sia una alimentazione PoE disponibile).

3.3.3. HPE Q9H62AFS-C

HPE Aruba AP 515

VANTAGGI

Con un numero crescente di dispositivi mobili e IoT (Internet of Things) che dipendono dall'accesso wireless, le reti devono gestire una mescolanza diversificata di tipi di dispositivi, applicazioni e servizi. Gli access point Campus Aruba serie 510 con tecnologia 802.11ax offrono in modo efficiente accesso a elevate prestazione a più client e tipi di traffico simultaneamente in ambienti in cui la densità è un problema, incrementando la velocità dei dati sia per i singoli dispositivi che per il sistema nel suo complesso. La serie 510 supporta velocità dati massime di 4,8 Gbps nella banda a 5 GHz e 575 Mbps nella banda a 2,4 GHz, ideale per ambienti ad alta densità come scuole, filiali retail, hotel e uffici aziendali.

Oltre alle funzionalità standard 802.11ax, la serie 510 supporta funzionalità quali la gestione delle radiofrequenze Aruba ClientMatch e le radiofrequenze aggiuntive per i servizi di localizzazione e le applicazioni IOT, offrendo un'esperienza utente ineguagliabile nell'ambiente digitale completamente wireless dei nostri giorni.

Componenti hardware fornite con bundle Aruba AP 515

- AP Q9H62A
- Power Injector R3K00A
- Cavo di alimentazione JW121A
- AP-MNT-D AP mount bracket
- N. 6 Antenne Dual-Band Omnidirezionali)

Efficienza migliorata

- Gli access point Campus Aruba serie 510 supportano più client simultaneamente e con grande efficienza, aumentando la velocità dei dati sia per i singoli dispositivi che per il sistema in generale.
- La trasmissione multiutente con OFDMA in downlink e uplink aumenta la velocità dei dati degli utenti e riduce la latenza, soprattutto per i moltissimi dispositivi con frame ridotti o bassi requisiti di velocità dei dati, come il traffico vocale e i dispositivi IoT.
- La funzionalità multiutente con MIMO multiutente downlink migliora la capacità della rete consentendo a più dispositivi di trasmettere simultaneamente.
- Dal momento che gli access point 802.11ax con prestazioni più elevate hanno un maggior consumo energetico, la funzione Aruba NetInsight GreenAP consente agli access point serie 510 di assorbire meno energia quando non vengono utilizzati, ad esempio di sera quando gli edifici sono vuoti.

Prestazioni elevate

- Con la tecnologia Aruba ClientMatch utilizzata negli access point Campus Aruba serie 510, si tenterà di raggruppare i dispositivi compatibili con lo standard 802.11ax sui trasmettitori AP con funzionalità equivalenti.
- I vantaggi prestazionali di OFDMA (Orthogonal Frequency Division Multiple Access) vengono massimizzati. Tutto ciò si traduce in migliori prestazioni di rete e nel potenziamento della sua capacità.
- La serie 510 utilizza ArubaOS 8 AirMatch (tecnologia di apprendimento automatico) per ottimizzare automaticamente le prestazioni della rete wireless regolando le frequenze radio (RF) degli access point.
- Gli access point girano su ArubaOS 8, offrendo una connessione di rete sempre disponibile attraverso funzionalità come LiveUpgrade, Controller Clustering e failover omogeneo.

Predisposizione per l'IoT

- Gli access point Campus Aruba serie 510 preparano la rete all'Internet of Things (IoT).

- La tecnologia 802.11ax offre vantaggi esclusivi per i dispositivi IoT, dai canali dedicati nella funzione OFDMA che consente la trasmissione simultanea delle connessioni IoT con bassa latenza, alle opzioni di risparmio energetico con Target Wake Time (TWT) per preservare la durata della batteria.
- La serie 510 supporta il collegamento radio integrato BLE (Bluetooth Low-Energy) e Zigbee, oltre a una porta USB per la massima flessibilità, offrendo una connettività sicura e affidabile per i dispositivi IOT e per l'implementazione dei servizi di localizzazione.

Access point dual radio 802.11ax

- Supporta fino a 4,8 Gbps nella banda a 5 GHz e 575 Mbps nella banda a 2,4 GHz (per una velocità massima aggregata di 5,4 Gbps).

Radio Bluetooth Low-Energy (BLE) integrata

- Abilita i servizi basati sulla posizione con i dispositivi mobili dotati di BLE che ricevono segnali da più Aruba Beacon contemporaneamente
- Consente la gestione di una rete di Aruba Beacon

ACC (Advanced Cellular Coexistence)

- Riduce al minimo l'interferenza generata da reti cellulari 3G/4G, sistemi di antenne distribuite e apparecchiature commerciali small cell/femtocell.

QoS per la visibilità e il controllo delle app

- Supporta la gestione delle priorità e l'applicazione delle politiche per app di comunicazioni unificate, tra cui Microsoft Skype for Business con dati crittografati di videoconferenze, voce, chat e condivisione di desktop

Aruba Air Slice™ per supporto OFDMA esteso

- Gli AP in modalità controller-less (Instant) possono fornire prestazioni SLA-grade assegnando RU a tipi di traffico specifici. Combinando il Policy Enforcement Firewall (PEF) di Aruba e la deep packet inspection (DPI) a Livello 7 per identificare il ruolo utente e applicazioni, gli AP assegneranno dinamicamente la larghezza di banda necessaria. Anche i client non Wi-Fi 6 possono trarne vantaggio.

Multi-user MIMO (MU-MIMO)

- Gli AP serie 510 supportano downlink mU-MIMO proprio come AP WiFi 5 (802.11ac Wave 2). Il vantaggio aggiunto è l'abilità di moltiplicare il numero di client che ora possono inviare traffico, ottimizzando così la diversità del flusso spaziale da client ad AP.

Ottimizzazione client consapevole Wi-Fi 6 e MU-MIMO

- Tecnologia ClientMatch basata su AI (Artificial Intelligence) brevettata da Aruba, elimina i problemi del client sticky agganciando i client Wi-Fi 6 al miglior AP disponibile. Vengono utilizzate le metriche della sessione per indirizzare i dispositivi mobili al miglior AP in base alla disponibilità larghezza di banda, tipi di applicazioni utilizzate e tipo di traffico anche mentre gli utenti sono in movimento.

Intelligent Power Monitoring (IPM)

- Gli AP Aruba monitorano e riportano continuamente il consumo di energia dell'hardware. Possono anche essere configurati per abilitare o disabilitare le funzionalità in base alla potenza PoE disponibile – ideale quando gli switch cablati hanno esaurito il loro budget di potenza.

Efficienza energetica AP verde

- Gli AP Wi-Fi 6 di Aruba utilizzano le analisi da NetInsight per attivare automaticamente una modalità di sospensione basata su densità del cliente.

Gestione RF

- La tecnologia Adaptive Radio Management (ARM) assegna automaticamente le impostazioni di canale e di potenza trasmissiva, fornisce airtime fairness e fa sì che gli AP operino senza fonti di interferenza RF per garantire WLAN affidabili e ad alte prestazioni
- Gli AP della serie 510 di Aruba possono essere configurati per fornire funzionalità di air monitoring part-time o dedicato per protezione dalle intrusioni wireless, tunnel VPN per estendere le sedi remote alle risorse aziendali e connessioni wireless mesh dove non siano disponibili cavi Ethernet

Visibilità e controllo intelligenti delle applicazioni

- La tecnologia AppRF si serve dell'esame approfondito dei pacchetti per classificare e bloccare, dare priorità o limitare la larghezza di banda per oltre 2.500 app aziendali o gruppi di app

Sicurezza

- La protezione dalle intrusioni wireless integrata protegge dalle minacce e le riduce, eliminando al contempo l'esigenza di sensori RF e applicazioni di sicurezza separate
- I servizi per la reputazione e la sicurezza dell'IP identificano, classificano e bloccano i file, gli URL e gli IP malevoli, fornendo una protezione avanzata dalle minacce online
- Tecnologia TPM (Integrated Trusted Platform Module) per l'archiviazione sicura di credenziali e chiavi

Ampia scelta delle modalità operative

- Gli AP della serie 510 di Aruba offrono una serie di modalità operative per soddisfare requisiti di gestione e installazione specifici.
- Modalità gestita da controller: quando sono gestiti tramite Mobility Controller di Aruba, gli AP Aruba della serie 510 offrono funzionalità di configurazione centralizzata, crittografia dei dati, applicazione delle politiche e servizi di rete, nonché inoltro distribuito e centralizzato del traffico
- Modalità Aruba Instant: in modalità Aruba Instant, un singolo AP distribuisce automaticamente la configurazione di rete agli altri AP Instant nella WLAN. Basta accendere un Instant AP, configurarlo via Wi-Fi e collegare gli altri AP: l'intera procedura richiede circa cinque minuti. Se i requisiti della WLAN cambiano, un percorso di migrazione integrato consente agli AP Instant della serie 510 di divenire parte di una WLAN gestita da un Mobility Controller
- AP remoto (RAP) per l'implementazione nelle filiali

- AM (Air Monitor) per IDS wireless, rilevamento e contenimento di server non autorizzati
- Analizzatore dello spettro, dedicato o ibrido, per l'identificazione delle fonti di interferenza RF
- Mesh aziendale sicura
- Per le installazioni di grandi dimensioni su più siti, il servizio Aruba Activate riduce notevolmente i tempi di installazione automatizzando il provisioning dei dispositivi, gli upgrade del firmware e la gestione dell'inventario. Con Aruba Activate, gli Instant AP sono spediti dallo stabilimento a qualsiasi sede e si configurano autonomamente all'accensione.

Specifiche

- AP Indoor, dual radio, 5GHz 802.11ax 4x4 MIMO e 2.4GHz 802.11ax 2x2 MIMO

Specifiche radio wi-fi

- Radio 5 GHz:
    - Quattro spatial stream Single User (SU) MIMO per una velocità massima di 4,8 Gbps per dispositivo client 802.11ax a 4SS HE160 (max)
    - Due spatial stream Single User (SU) MIMO per una velocità massima di 1,2 Gbps per dispositivo client 802.11ax (max) a 2SS HE80 (tipico)
    - Quattro spatial stream Multi User (MU) MIMO per una velocità massima di 4,8 Gbps fino a 4 dispositivi client 1SS o due dispositivi client 2SS HE160 802.11ax DL-MU-MIMO contemporaneamente (max)
    - Quattro spatial stream Multi User (MU) MIMO per una velocità massima di 2,4 Gbps fino a 4 dispositivi client 1SS o due dispositivi client 2SS HE80 802.11ax DL-MU-MIMO contemporaneamente (tipico)
- Radio 2,4 GHz:
- Due spatial stream Single User (SU) MIMO per una velocità massima di 574 Mbps per dispositivo client 802.11ax a 1SS HE40 o due dispositivi client 802.11ax 1SS HE40 DL-MU-MIMO simultaneamente (max)
    - Due spatial stream Single User (SU) MIMO per una velocità massima di 287 Mbps per dispositivo client 802.11ax a 2SS HE20 o due dispositivi client 802.11ax 1SS HE20 DL-MU-MIMO simultaneamente (tipico)
- Dual radio configurabile tramite software, supporta 5 GHz (Radio 0) e 2,4 GHz (Radio 1)
- Supporto di un massimo di 512 dispositivi client associati per radio e di massimo 16 BSSID per radio
- Bande di frequenze supportate (si applicano restrizioni specifiche di singoli paesi):
    - Da 2,400 a 2,4835 GHz
    - Da 5,150 a 5,250 GHz
    - Da 5,250 a 5,350 GHz
    - Da 5,470 a 5,725 GHz
    - Da 5,725 a 5,850 GHz

- Canali disponibili: a seconda del dominio regolatore configurato
- La selezione dinamica delle frequenze (DFS, Dynamic Frequency Selection) ottimizza l'utilizzo dello spettro RF disponibile
- Tecnologie radio supportate:
    - 802.11b: Direct-sequence spread-spectrum (DSSS)
    - 802.11a/g/n/ac: Orthogonal frequency-division multiplexing (OFDM)
    - 802.11ax: Orthogonal frequency-division multiple access (OFDMA) con fino a 16 resource units (per un canale da 80MHz)
- Tipi di modulazione supportati:
    - 802.11b: BPSK, QPSK, CCK
    - 802.11a/g/n/ac: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM, 1024-QAM (estensione proprietaria)
    - 802.11ax: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM, 1024-QAM
- Potenza di trasmissione: configurabile in incrementi di 0,5 dBm
- Potenza di trasmissione massima (condotta), limitata da requisiti normativi locali:
    - Banda 2,4 GHz: +18 dBm per chain, +21 dBm aggregata
    - Banda 5GHz: +18 dBm per chain, +24 dBm aggregata
    - Nota: i livelli di potenza di trasmissione condotta escludono il guadagno dell'antenna. Per la potenza di trasmissione (EIRP) massima, aggiungere il guadagno dell'antenna
- La funzionalità ACC (Advanced Cellular Coexistence) riduce al minimo l'interferenza generata dalle reti cellulari
- Tecnologia MRC (Maximum Ratio Combining) per prestazioni del ricevitore ottimizzate
- Tecnologia CDD/CSD (Cyclic Delay/Shift Diversity) per prestazioni RF in downlink ottimizzate
- Intervallo di guardia breve per i canali a 20 MHz, 40 MHz, 80MHz e 80 MHz
- Codifica STBC (Space-Time Block Coding) per un maggiore intervallo e una ricezione ottimizzata
- Tecnologia LDPC (Low-Density Parity Check) per una correzione degli errori ad alta efficienza e un throughput più elevato
- Beamforming di trasmissione (TxBF) per una migliore affidabilità e raggio del segnale
- 802.11ax Target Wait Time (TWT) per supporto a dispositivi low-power
- Velocità dei dati supportate (Mbps):
    - 802.11b: 1, 2, 5,5, 11
    - 802.11a/g: 6, 9, 12, 18, 24, 36, 48, 54
    - 802.11n (2.4GHz): da 6.5 a 300 (da MCS0 a MCS15, da HT20 a HT40)
    - 802.11n (5GHz): da 6.5 a 600 (da MCS0 a MVC31, da HT20 a HT40)

  - 802.11ac: da 6.5 a 3,467 (da MCS0 a MCS9, NSS = da 1 a 4, da VHT20 a VHT160)
  - 802.11ax (2.4GHz): da 3.6 a 574 (da MCS0 a MCS11, NSS = da 1 a 2, da HE20 a HE40)
  - 802.11ax (5GHz): da 3.6 a 4,803 (da MCS0 a MCS11, NSS = da 1 a 4, da HE20 a HE160)
- Supporto 802.11n High-Throughput (HT): HT 20/40
- Supporto 802.11ac VHT: VHT 20/40/80/160
- 802.11ax high efficiency (HE) support: HE20/40/80/160
- Aggregazione pacchetti 802.11n/ac: A-MPDU, A-MSDU

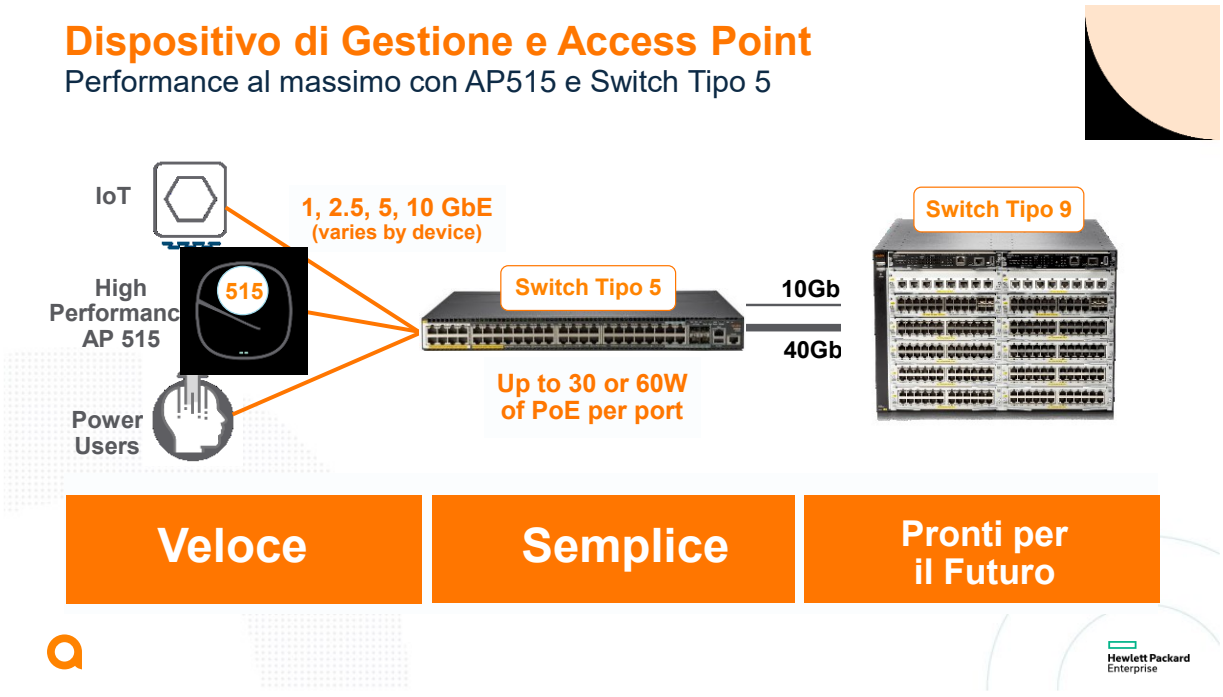
Antenne wi-fi

- Quattro antenne omnidirezionali integrate dual-band downtilt per MIMO 4x4 con guadagno massimo dell'antenna di 4,2 dBi a 2,4GHz e 7,5dBi a 5GHz. Le antenne integrate sono ottimizzate per il montaggio orizzontale a soffitto dell'AP. L'angolo downtilt per il guadagno massimo è di circa 30 gradi.

  Il guadagno massimo dei modelli di antenna combinati (sommati) per tutti gli elementi che operano sulla stessa banda è di 3,8 dBi a 2,4 GHz e 4,6 dBi a 5 GHz

Altre interfacce

- E0: porta HPE SmartRate (RJ-45, massima velocità negoziata 2,5 Gbps)
  - Velocità collegamento auto-sensing (100/1000 / 2500BASE-T) e MDI / MDX
  - La velocità di 2,5 Gbps è conforme a NBase-T e Specifiche 802.3bz
  - PoE-PD: 48Vdc (nominale) 802.3af / at / bt (classe 3 o superiore)
  - 802.3az Energy Efficient Ethernet (EEE)



Veloci verso il futuro con IEEE802.3bz (SmartRate)

- E1: interfaccia di rete Ethernet 10/100 / 1000BASE-T (RJ-45)
    - Velocità di collegamento con rilevamento automatico e MDI / MDX
    - 802.3az Energy Efficient Ethernet (EEE)
- Supporto di aggregazione dei collegamenti (LACP) tra le due porte per ridondanza e maggiore capacità
- Interfaccia di alimentazione CC: 12Vcc (nominale, +/- 5%), accetta interruttore circolare positivo al centro da 2,1 mm / 5,5 mm con lunghezza 9,5 mm
- Interfaccia host USB 2.0 (connettore di tipo A)
- Capacità di approvvigionamento fino a 1A / 5W su un dispositivo collegato
- Radio Bluetooth 5 e Zigbee (802.15.4) (2.4GHz)
    - Bluetooth 5: potenza di trasmissione fino a 8 dBm (classe 1) e sensitività di ricezione -95dBm
    - Zigbee: fino a 8 dBm di potenza di trasmissione e -97 dBm sensitività di ricezione
    - Antenna omnidirezionale polarizzata verticalmente integrata con una inclinazione di circa 30 gradi e un guadagno di picco di 3,5 dBi
- Indicatori visivi (due LED multicolori): per sistema e stato della radio
- Pulsante di ripristino: ripristino delle impostazioni di fabbrica, controllo modalità LED (normale / spento)
- Interfaccia console seriale (proprietaria, micro-B USB jack fisico)
- Slot di sicurezza Kensington

Sorgenti di alimentazione e consumo

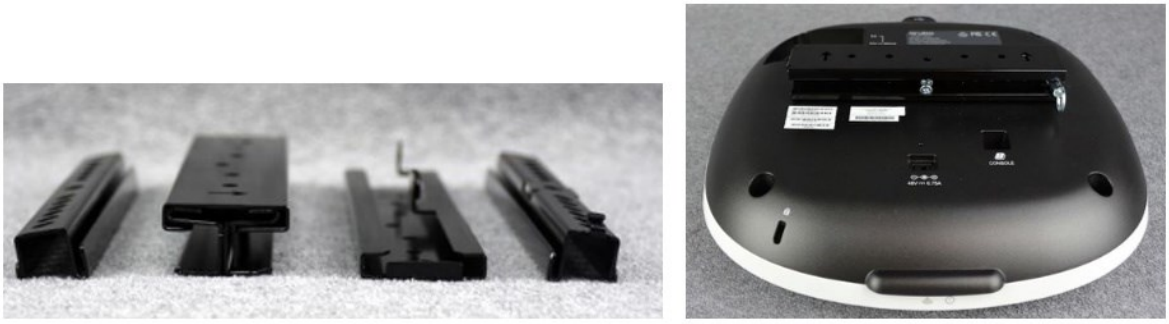
- L'AP supporta l'alimentazione DC diretta e l'alimentazione Ethernet (PoE; sulla porta E0)
- Quando sono disponibili entrambe le fonti di alimentazione, l'alimentazione in corrente continua ha priorità rispetto alla PoE
- Gli alimentatori sono venduti separatamente;
- Se alimentato da DC o 802.3at (classe 4) / 802.3bt (classe 5) PoE, l'AP funzionerà senza restrizioni.
- Se alimentato da PoE 802.3af (classe 3) e con funzione IPM abilitata, l'AP verrà avviato in modalità illimitata, ma può applicare restrizioni a seconda del budget della PoE e della potenza reale. È possibile programmare quali restrizioni IPM applicare e in quale ordine.
- Funzionamento dell'AP con un PoE 802.3af (classe 3 o inferiore) sorgente e IPM disabilitati non sono supportati.
- Consumo energetico massimo (nel caso peggiore):
    - Alimentazione DC: 16,0 W.
    - Alimentazione PoE (802.3af, IPM abilitato): 13,5 W.

  - Alimentazione PoE (802.3at / bt): 20,8 W.
- Tutti i numeri sopra indicati sono privi di un dispositivo USB esterno collegato. Quando si sfrutta l'intero budget di potenza di 5W per tale dispositivo, si incrementa (nel caso peggiore) il consumo per l'AP fino a 5,7 W (alimentazione PoE) o 5,5 W (alimentazione CC).
- Consumo energetico massimo (nel caso peggiore) in modalità inattiva: 12,6 W (PoE) o 9,7 W (DC)
- Consumo energetico massimo (nel peggiore dei casi) in condizioni di modalità deep-sleep: 5,9 W (PoE) o 1,5 W (DC).

Montaggio

L'AP viene fornito in dotazione con staffa di montaggio su parete/superfice solida (colore nero

- Mount kit fornito nel Bundle di convenzione:
- AP-MNT-D



HPE Aruba AP-MNT-D

Caratteristiche fisiche

- Dimensioni/peso dell'unità esclusi gli accessori di montaggio:
  - 200mm x 200mm x 46mm / 810g
- Dimensioni/peso (confezione di spedizione): •190mm x 180mm x 70mm / 590g

Condizioni ambientali

- Funzionamento:
  - Temperatura: da 0 ° C a + 50 ° C
  - Umidità: dal 5% al 93% senza condensa
  - AP è assemblato (plenum) per l'uso negli spazi di trattamento dell'aria
  - Ambienti ETS 300 019 classe 3.2
- Immagazzinaggio e trasporto:
  - Temperatura: da 40°C a +70°C

- Umidità: dal 5% al 93% senza condensa
- Ambienti ETS 300 019 classi 1.2 e 2.3

Conformità normativa

- FCC / ISED
- Marchio CE
- Direttiva RED 2014/53 / UE
- Direttiva EMC 2014/30 / UE
- Direttiva bassa tensione 2014/35 / UE
- UL / IEC / EN 60950
- EN 60601-1-1, EN60601-1-2

Certificazioni

- Plenum UL2043
- Wi-Fi Alliance:
  - Wi-Fi CERTIFIED a, b, g, n, ac, ax
  - WPA, WPA2 e WPA3 - Enterprise con opzione CNSA, Personal (SAE), Enhanced Open (OWE)
  - WMM, WMM-PS, Wi-Fi Vantage, W-Fi Agile Multiband
  - Passpoint (versione 2)
- Bluetooth SIG

Garanzia

- Garanzia a vita limitata Aruba

Versioni minime del software

- ArubaOS 8.4.0.0
- Aruba InstantOS 8.4.0.0

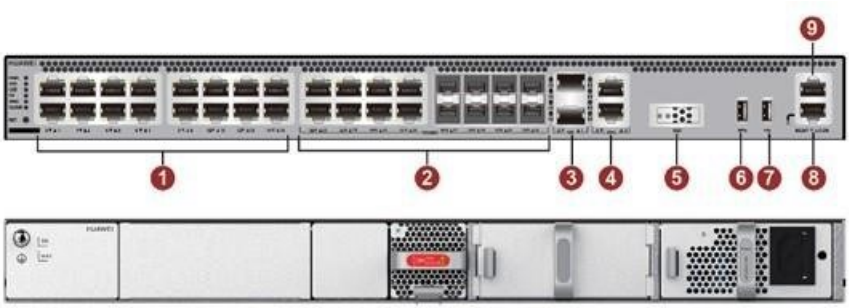
Per maggiori Informazioni e per una documentazione esaustiva in merito ai prodotti e la guida utile alla configurazione, si rimanda al seguente link: Aruba Network Architecture WiFi

4. Dispositivi per la sicurezza delle reti

4.1. Dispositivi di sicurezza fascia base

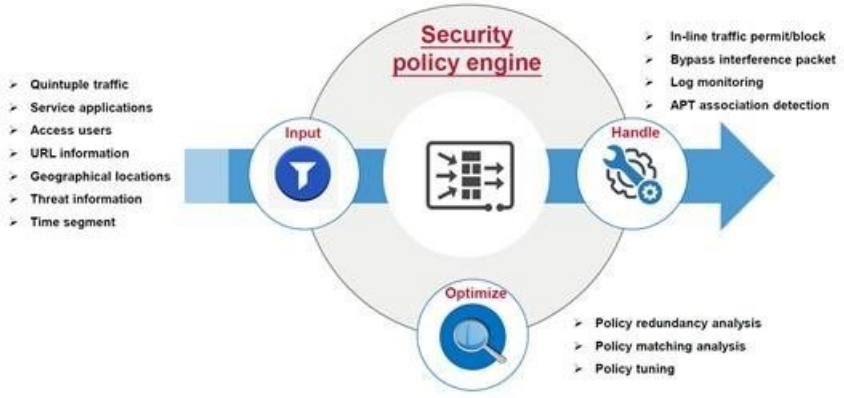
4.1.1. Huawei USG6515E

Il modello USG6515E è il modello base della famiglia dei HiSecEngine Next Generation Firewall USG6500E. È un appliance UTM a configurazione fissa con integrate 8 Gigabit Ethernet Combo (RJ45 o SFP) + 16 interfacce GE rame e 2 interfacce 10GE (SFP+), di altezza 1 RU (con possibilità d'installazione a rack tramite opportuno kit, fornito) ed alimentazione ridondata in AC. In dotazione di Convenzione, è fornito con doppio alimentatore e un SSD da 64GB.

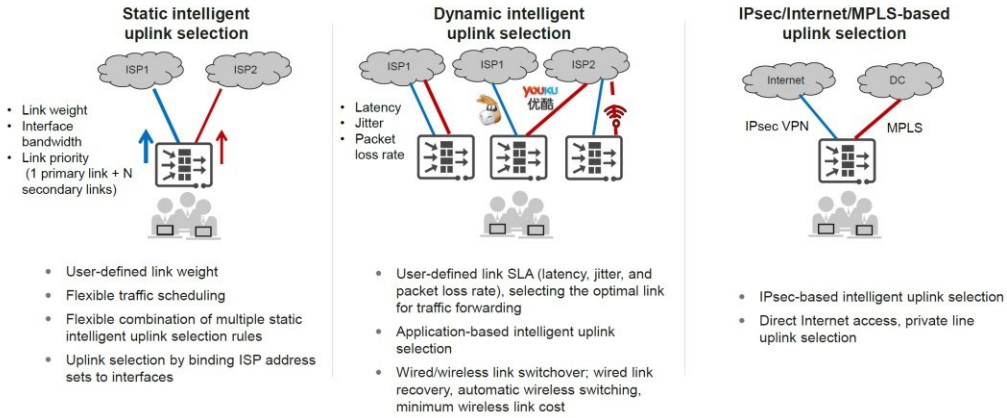


1. 16 x GE (RJ45)
2. 8 x GE (Combo)
3. 2 x 10GE (SFP+)
4. 2 x WAN port
5. SSD card slot
6. 1 x USB3.0
7. 1 x USB2.0
8. 1 x GE (RJ45) management port
9. Console port

Come tutti i modelli della famiglia, è un apparato multi purpose che integra funzionalità di Application Firewall, VPN (IPSec, SSL, L2TP, Dymanic Smart VPN e fornito con il Huawei-developed VPN client Secoclient per SSL SSL VPN, L2TP VPN e L2TP over IPSec VPN remote access), IPS (up-to-date threat information), Antivirus (5 milioni di Virus/Troyan con database aggiornato quotidiamente), Data Leak Prevention (identificazione e filtro su oltre 120 tipi di files e contenuto), SSL-encrypted traffic detection, Anti-DDOS (più di 10 tipi di attacchi DDos), Application Control and Application-based Bandwidth management (sul base utente) e Url filtering (predefined URL category database da 85 milioni di URL).



Supporta funzionalità avanzate di Routing (IP, OSPF, BGP, IS-IS, RIPng, OSPFv3, BGP4+, IPv6 IS-IS), di alta affidabilità (hot standby in active/standby and load balancing, link backup o link group, BFP, VRRP) e di Intelligent uplink selection.



È possibile dispiegarlo in configurazione di alta affidabilità (active/active e active/standby) e in modalità routed come transparent mode (in quest'ultima è inclusa anche il "virtual wire"). Di default (senza licenza aggiuntiva) supporta 10 Virtual Context e 100 SSL VPN users. L'apparato ha un throughput Firewall fino a 2Gbps e prestazioni, con tutti i servizi attivi (FW + SA + IPS + Antivirus Throughput) fino a 1,5 Gbps.

Certificato: NSS Labs

È gestibile (configurazione, monitoraggio e allarmistica) dal sistema di management eSight (Tipo 10) incluso all'interno della Convenzione.

4.1.2. Fortinet FG-60E-BDL-950-12

In fase di sostituzione per End of Sale

4.1.3. Checkpoint CPAP-SG750-NGTP

In fase di sostituzione per End of Sale

4.2. Dispositivi di sicurezza fascia media

4.2.1. Huawei USG6620-C

In fase di sostituzione per End of Sale

4.2.2. Fortinet FG-200E-BDL-950-12

L'apparato proposto come dispositivo per la sicurezza di fascia media è il FortiGate 200E, che offre una eccellente e flessibile soluzione di sicurezza per la protezione di aziende di medie dimensioni, dotata di processori dedicati ad alte prestazioni che elaborano i servizi di NGFW garantendo performance, efficacia e visibilità dello stato di sicurezza della rete.

Di seguito sono riportati i requisiti minimi e migliorativi richiesti nella gara per i dispositivi di fascia media.

Requisiti minimi per i dispositivi di sicurezza di fascia media:

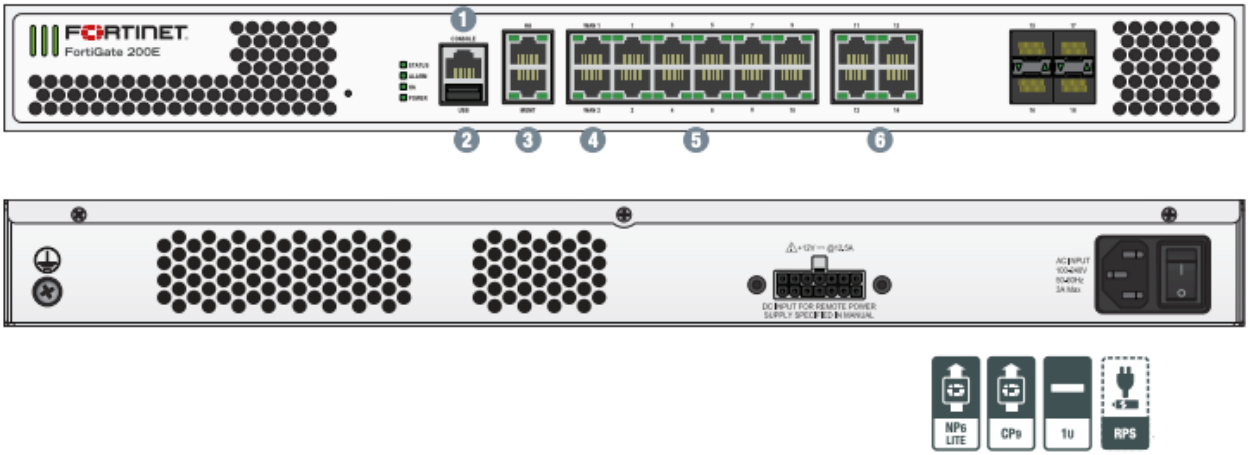
- Funzionalità Antivirus
- Funzionalità di Application Control
- Funzionalità di Intrusion Prevention System (IPS)
- Funzionalità Firewall
- VPN IPSec
- Funzionalità web/url filtering
- Almeno 8 interfacce 1000Base-T
- Almeno 2 interfacce Gigabit Ethernet SFP o SFP+ - esclusi i transceiver
- IPS throughput almeno pari a 2 Gbps
- Firewall throughput almeno pari a 6 Gbps
- VPN throughput almeno pari a 1 Gbps
- Almeno 2 milioni di sessioni contemporanee

- Almeno 40.000 nuove sessioni al secondo

Caratteristiche migliorative per i dispositivi di sicurezza di fascia media:

- Funzionalità antispam
- Meccanismi di rilevazione e protezione per attacchi di tipo Denial of Service
- Almeno 2 ulteriori interfacce Gigabit Ethernet SFP o SFP+ - esclusi i transceiver
- Funzionalità di TLS o SSL Inspection
- Supporto per configurazioni High Availability
- Funzionalità VPN TLS o SSL
- Supporto IPv6
- Funzionalità di traffic shaping (gestione QoS)
- Presenza di almeno 10 contesti virtuali
- Miglioramento di almeno il 30% delle prestazioni minime previste per l'Intrusion Prevention throughput (2,6 Gbps)
- Miglioramento di almeno il 30% delle prestazioni minime previste per Firewall throughput (7,8 Gbps)
- Miglioramento di almeno il 30% delle prestazioni minime previste per VPN throughput (1,3 Gbps)
- Miglioramento di almeno il 30% delle prestazioni minime previste per il numero di sessioni contemporanee (2,6 M)
- Miglioramento di almeno il 30% delle prestazioni minime previste per il numero di nuove sessioni al secondo (52.000)

Il Fortigate 200E è un appliance di fascia media enterprise che soddisfa i requisiti sia minimi che migliorativi di gara.



Interfaces

1. Console Port
2. USB Port
3. 2x GE RJ45 Management/HA Ports
4. 2x GE RJ45 WAN Ports
5. 14x GE RJ45 Ports
6. 4x GE SFP Slots

Questo dispositivo è dotato di 18 interfacce 1000 base-T, di cui due dedicate al collegamento WAN, due interfacce 1000 base-T dedicate al management/HA e 4 slot SFP. Il sistema viene offerto completo di subscription Fortiguard UTP (Unified Threat Protection) per i servizi di Application Control, IPS, AV (AntiMalware Protection), Web Filtering ed Antispam.

Il FortiGate 200E dispone del sistema operativo FortiOS comune a tutte le piattaforme di firewall Fortinet. Il sistema operativo FortiOS fornisce all'utente un elevato numero di funzionalità aggiuntive incluse nell'offerta senza necessità di ulteriori subscription. In particolare, all'interno del pacchetto base sono presenti tutte le funzionalità necessarie all'implementazione semplice e sicura di architetture SD-WAN. L'implementazione Secure SD-WAN del FortiOS garantisce un controllo intelligente dei percorsi su rete WAN, con o senza overlay IP-SEC, utilizzando più di 3000 applicazioni o utenti/gruppi per gestire le metriche di qualità della rete ed implementando politiche di routing e bandwidth management con l'utilizzo delle funzionalità di Quality of Service e Traffic Shaping.

Il livello di subscription fornito garantisce l'accesso anche alle seguenti funzionalità:

- Funzionalità FortiOS
    - SSL Inspection
    - SD-WAN
    - Routing e NAT con supporto per la Traffic Redirection con ICAP (Internet Content Adaptation Protocol)
    - L2 Switching (con supporto VXLAN e EMAC)
    - Explicit Proxy
    - Quality of Service (QoS) e Traffic Shaping
    - Data leak prevention (DLP)

    - Controller integrato per FortiSwitch e FortiWiFi
- FortiCare; include Internet Service DB, Client ID DB, IP Geography DB, Malicious URL DB, URL Whitelist DB
- Estensione del servizio AV - Advanced Malware Protection (AMP)
    - Mobile Malware Security; per proteggere i client dalle minacce destinate a device mobili. La subscription include le funzionalità di mobile application control e protezione antimalware per piattaforme Apple IOS ed Android
    - Botnet
    - Content Disarm and Reconstruction (CDR); per rimuovere gli allegati malevoli e sostituirli con un file "disarmato"
    - Virus Outbreak Protection; servizio di verifica delle firme antivirus in tempo reale.
- DNS Filtering: il servizio permette di filtrare direttamente le query DNS per evitare traffico http verso domini compromessi
- FortiSandbox Cloud Service; servizio che permette di massimizzare la protezione dalle minacce 0-day e identificare un attacco sulla base di tecniche di analisi avanzata e sandboxing. Il servizio, richiesto in gara è già disponibile nel bundle dei servizi e non è soggetto a costi aggiuntivi.

La tabella seguente fornisce un dettaglio delle specifiche tecniche e prestazionali della macchina:

Specifiche hardware	
Interfacce GE RJ45	14 (+2 WAN) (+2 MGT/HA)
GE SFP Slots	4
Porte Console (RJ45)	1
Porte USB	1
Performance di Sistema	
Firewall Throughput (1518 / 512 / 64 byte, UDP)	20 / 20 / 9 Gbps
Latenza Firewall (64 byte UDP packets)	3 µs
Firewall Throughput (Pacchetti per Secondo)	13.5 Mpps

IPS Throughput (Enterprise Mix)	2.2 Gbps
IPS Throughput (http)	2.6 Gbps
Sessioni Concorrenti (TCP)	2.6 Million
Nuove Sessioni/Secondo (TCP)	135,000
Firewall Policies	10,000
IPsec VPN Throughput (512 byte)	7.2 Gbps
Gateway-to-Gateway IPsec VPN Tunnels	2,000
Client-to-Gateway IPsec VPN Tunnels	10,000
SSL-VPN Throughput	900 Mbps
Utenti SSL Concorrenti (Massimo raccomandato, tunnel mode)	500
SSL Inspection Throughput (IPS, HTTP)	820 Mbps
Sessioni Concorrenti SSL Inspection (IPS, avg. HTTPS)	240.000
Application Control Throughput (HTTP 64K)	3.5 Gbps
CAPWAP Throughput (1444 byte, UDP)	1.5 Gbps
Virtual Domains (Default / Maximum)	10/10
Numero Massimo di FortiSwitches Supportati	64
Numero Massimo di FortiAPs (Totali / Tunnel Mode)	256 / 128
Numero Massimo di FortiTokens	5,000

Configurazioni di High Availability	Active/Active, Active/Passive, Clustering
Dimensioni	
Altezza x Larghezza x Lunghezza (mm)	44.45 x 432 x 301
Peso	5.4 kg
Form Factor	1 RU

Riferimenti documentali pubblici:
https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_200E_Series.pdf

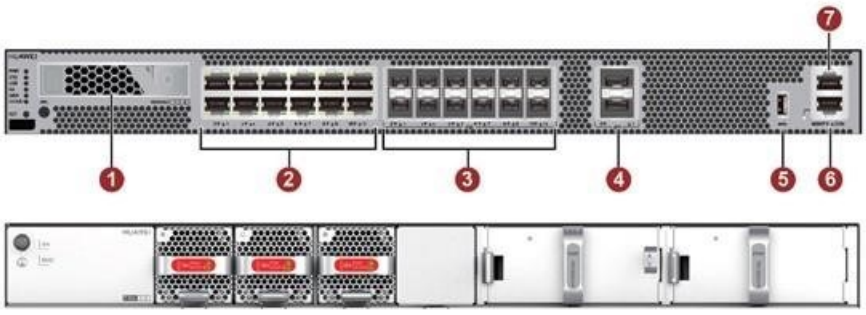
4.2.3. Checkpoint CPAP-SG5400-NGTP

In fase di sostituzione per End of Sale

4.3. Dispositivi di sicurezza fascia alta

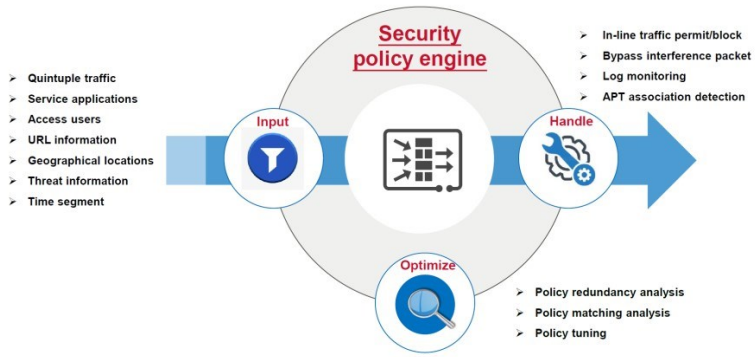
4.3.1. Huawei USG6630E

Il modello USG6630E è un modello della famiglia dei HiSecEngine Next Generation Firewall USG6600E. È un appliance UTM a configurazione fissa con integrate 12 interfacce 10GE (SFP+) (che lavorano a 1GE) + 12 interfacce GE rame e 2 interfacce 40GE (QSFP+), di altezza 1 RU (con possibilità d'installazione a rack tramite opportuno kit, fornito) ed alimentazione ridondata in AC. In dotazione di Convenzione, è fornito con doppio alimentatore e un SSD da 240GB.

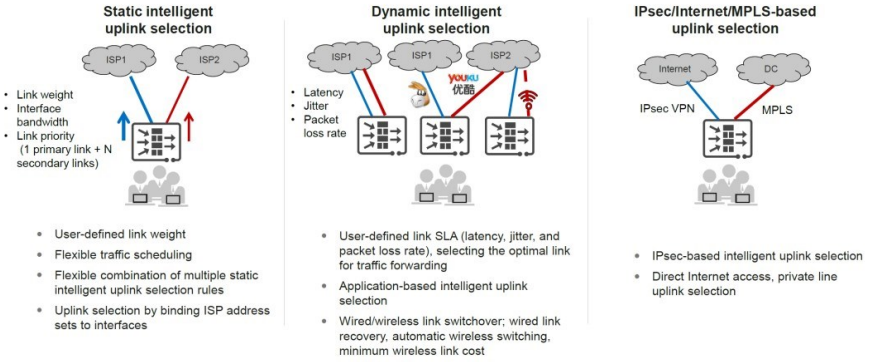


1. HDD/SSD Slot
2. 12 x GE (RJ45)
3. 12 x 10GE (SFP+)
4. 2 x 40GE (QSFP+)
5. 1 x USB3.0
6. 1 x GE (RJ45) management port
7. Console port

Come tutti i modelli della famiglia, è un apparato multi purpose che integra funzionalità di Application Firewall, VPN (IPSec, SSL, L2TP, Dymanic Smart VPN e fornito con il Huawei-developed VPN client Secoclient per SSL SSL VPN, L2TP VPN e L2TP over IPSec VPN remote access), IPS (up-to-date threat information), Antivirus (5 milioni di Virus/Troyan con database aggiornato quotidianamente), Data Leak Prevention (identificazione e filtro su oltre 120 tipi di files e contenuto), SSL-encrypted traffic detection, Anti-DDOS (più di 10 tipi di attacchi DDos), Application Control and Application-based Bandwidth management (sul base utente) e Url filtering (predefined URL category database da 85 milioni di URL).

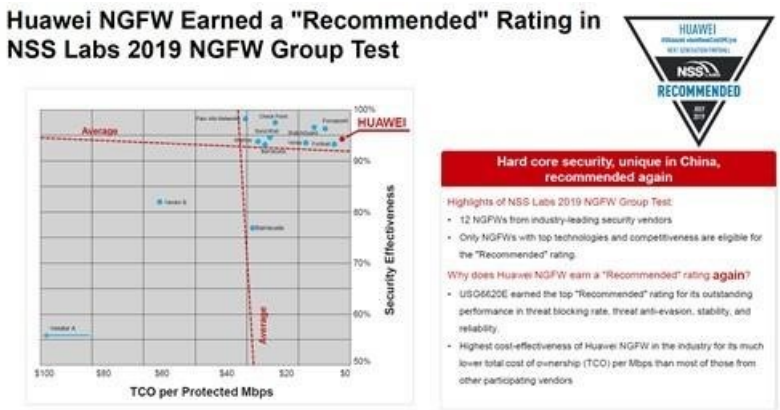


Supporta funzionalità avanzate di Routing (IP, OSPF, BGP, IS-IS, RIPng, OSPFv3, BGP4+, IPv6 IS-IS), di alta affidabilità (hot standby in active/standby and load balancing, link backup o link group, BFP, VRRP) e di Intelligent uplink selection.



È possibile dispiegarlo in configurazione di alta affidabilità (active/active e active/standby) e in modalità routed come transparent mode (in quest'ultima è inclusa anche il "virtual wire").

Di default (senza licenza aggiuntiva) supporta 10 Virtual Context e 100 SSL VPN users. L'apparato ha un throughput Firewall fino a 30Gbps e prestazioni, con tutti i servizi attivi (FW + SA + IPS + Antivirus Throughput) fino a 12 Gbps.



Certificato: NSS Labs

È gestibile (configurazione, monitoraggio e allarmistica) dal sistema di management eSight (Tipo 10) incluso all'interno della Convenzione.

4.3.2. Fortinet FG-500E-BDL-950-12

In fase di sostituzione per End of Sale

4.3.3. Checkpoint CPAP-SG5800-NGTP-HPP

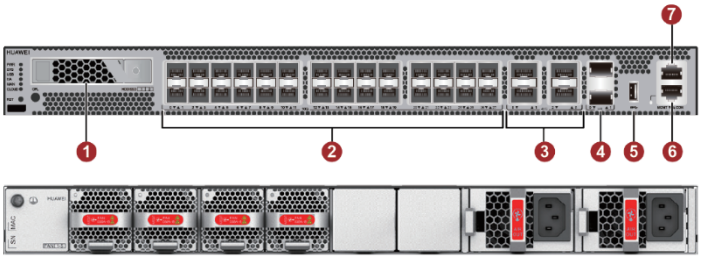
In fase di sostituzione per End of Sale

4.4. Dispositivi di sicurezza fascia top

4.4.1. Huawei USG6680E

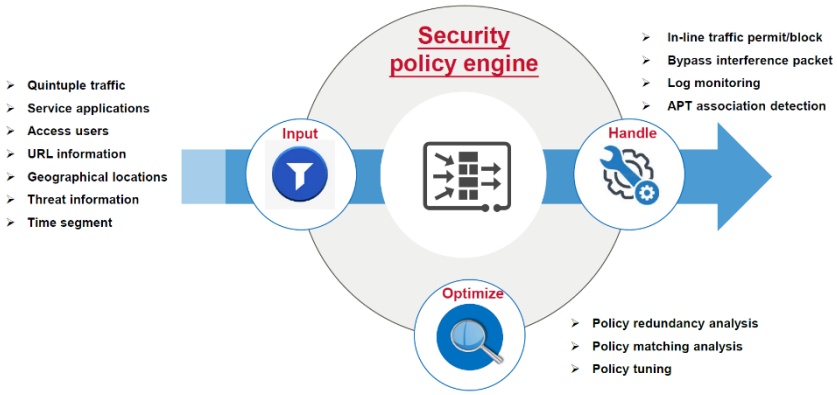
Il modello USG6680E è un modello della famiglia dei HiSecEngine Next Generation Firewall USG6600E. È un appliance UTM a configurazione fissa con integrate 28 interfacce 10GE (SFP+) (che lavorano a 1GE) + 4 interfacce 40GE (QSFP+), di altezza 1 RU (con possibilità d'installazione a rack tramite opportuno kit, fornito) ed alimentazione ridondata in AC. In dotazione di Convenzione, è fornito con doppio alimentatore e un SSD da 240GB.

USG6680E

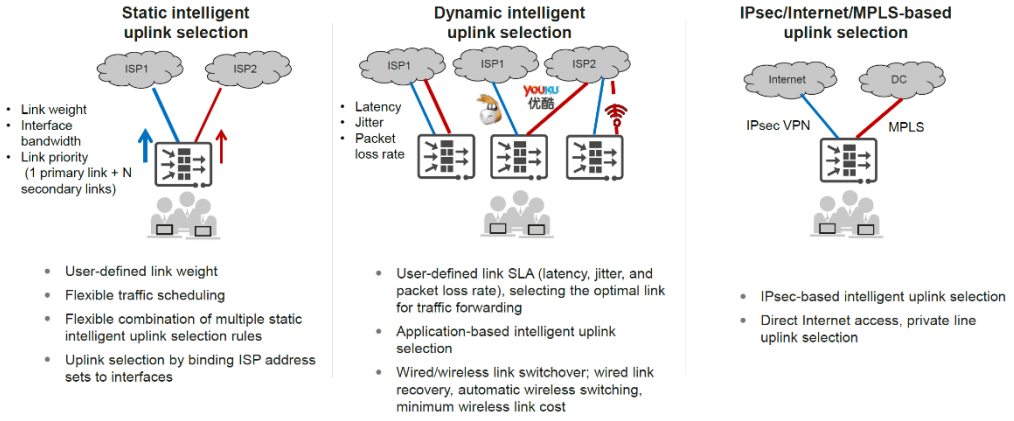


1. HDD/SSD Slot
2. 28 x10 GE (SFP+)
3. 4 x 40GE (QSFP+)
4. 2 x HA (SFP+)
5. 1 x USB3.0
6. 1 x GE (RJ45) management port
7. Console port

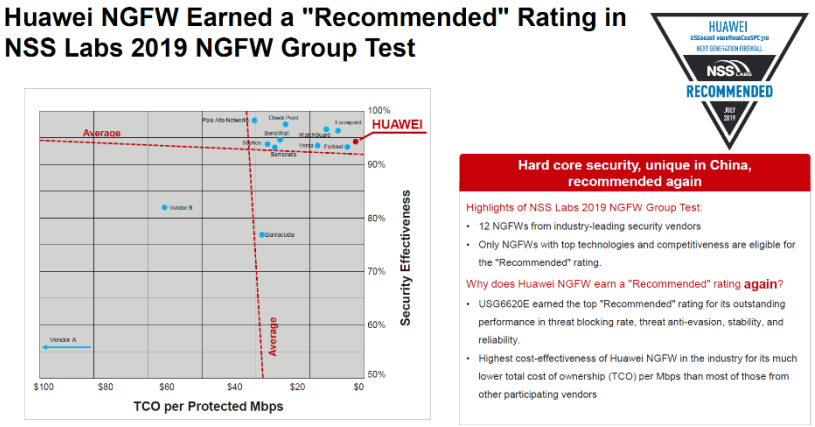
Come tutti i modelli della famiglia, è un apparato multi purpose che integra funzionalità di Application Firewall, VPN (IPSec, SSL, L2TP, Dymanic Smart VPN e fornito con il Huawei-developed VPN client Secoclient per SSL SSL VPN, L2TP VPN e L2TP over IPSec VPN remote access), IPS (up-to-date threat information), Antivirus (5 milioni di Virus/Troyan con database aggiornato quotidianamente), Data Leak Prevention (identificazione e filtro su oltre 120 tipi di files e contenuto), SSL-encrypted traffic detection, Anti-DDOS (più di 10 tipi di attacchi DDos), Application Control and Application-based Bandwidth management (sul base utente) e Url filtering (predefined URL category database da 85 milioni di URL).



Supporta funzionalità avanzate di Routing (IP, OSPF, BGP, IS-IS, RIPng, OSPFv3, BGP4+, IPv6 IS-IS), di alta affidabilità (hot standby in active/standby and load balancing, link backup o link group, BFP, VRRP) e di Intelligent uplink selection.



È possibile dispiegarlo in configurazione di alta affidabilità (active/active e active/standby) e in modalità routed come transparent mode (in quest'ultima è inclusa anche il "virtual wire"). Di default (senza licenza aggiuntiva) supporta 10 Virtual Context e 100 SSL VPN users. L'apparato ha un throughput Firewall fino a 80Gbps e prestazioni, con tutti i servizi attivi (FW + SA + IPS + Antivirus Throughput) fino a 23 Gbps.



Certificato: NSS Labs

È gestibile (configurazione, monitoraggio e allaramistica) dal sistema di management eSight (Tipo 10) incluso all'interno della Convenzione.

4.4.2. Fortinet FG-1500D-BDL-950-12

In fase di sostituzione per End of Sale

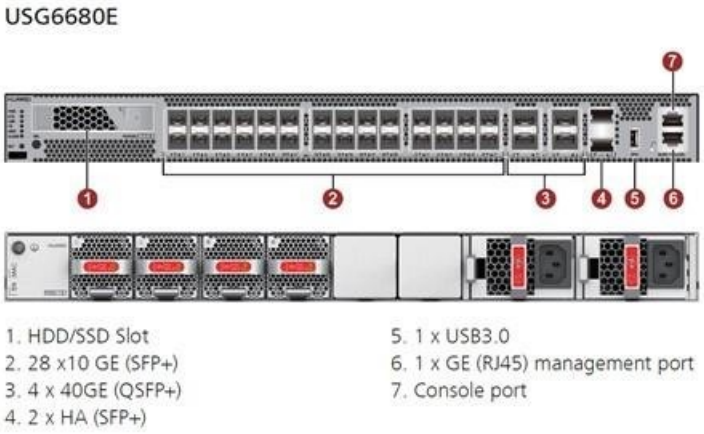
4.4.3. Checkpoint CPAP-SG15400-NGTP-HPPVS10

In fase di sostituzione per End of Sale

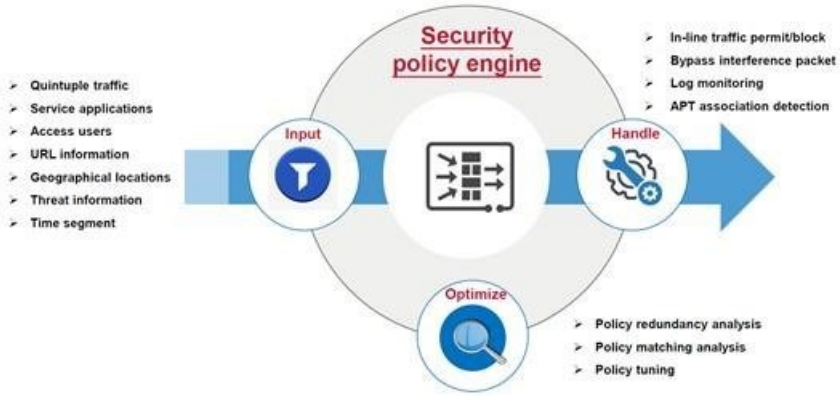
4.5. Dispositivi di sicurezza fascia enterprise

4.5.1. Huawei USG6680E

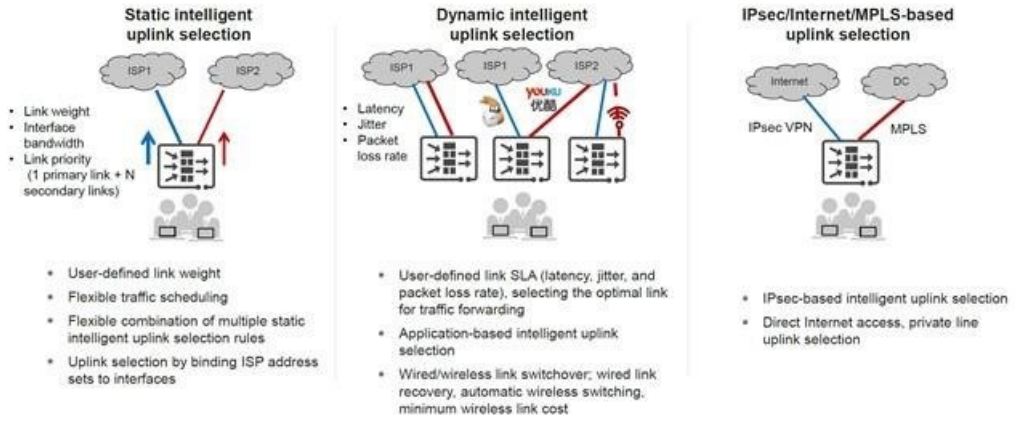
Il modello USG6680E è un modello della famiglia dei HiSecEngine Next Generation Firewall USG6600E. È un appliance UTM a configurazione fissa con integrate 28 interfacce 10GE (SFP+) (che lavorano a 1GE) + 4 interfacce 40GE (QSFP+), di altezza 1 RU (con possibilità d'installazione a rack tramite opportuno kit, fornito) ed alimentazione ridondata in AC. In dotazione di Convenzione, è fornito con doppio alimentatore e un SSD da 240GB.



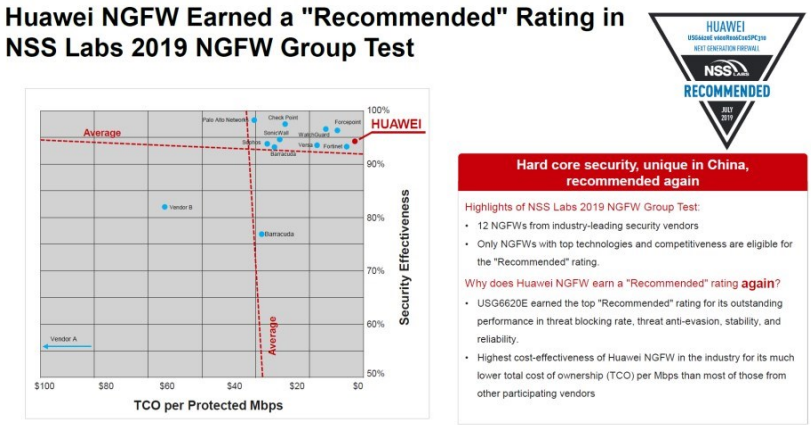
Come tutti i modelli della famiglia, è un apparato multi purpose che integra funzionalità di Application Firewall, VPN (IPSec, SSL, L2TP, Dymanic Smart VPN e fornito con il Huawei-developed VPN client Secoclient per SSL SSL VPN, L2TP VPN e L2TP over IPSec VPN remote access), IPS (up-to-date threat information), Antivirus (5 milioni di Virus/Troyan con database aggiornato quotidianamente), Data Leak Prevention (identificazione e filtro su oltre 120 tipi di files e contenuto), SSL-encrypted traffic detection, Anti-DDOS (più di 10 tipi di attacchi DDos), Application Control and Application-based Bandwidth management (sul base utente) e Url filtering (predefined URL category database da 85 milioni di URL).



Supporta funzionalità avanzate di Routing (IP, OSPF, BGP, IS-IS, RIPng, OSPFv3, BGP4+, IPv6 IS-IS), di alta affidabilità (hot standby in active/standby and load balancing, link backup o link group, BFP, VRRP) e di Intelligent uplink selection.



È possibile dispiegarlo in configurazione di alta affidabilità (active/active e active/standby) e in modalità routed come transparent mode (in quest'ultima è inclusa anche il "virtual wire"). Di default (senza licenza aggiuntiva) supporta 10 Virtual Context e 100 SSL VPN users. L'apparato ha un throughput Firewall fino a 80Gbps e prestazioni, con tutti i servizi attivi (FW + SA + IPS + Antivirus Throughput) fino a 23 Gbps.



Certificato: NSS Labs

È gestibile (configurazione, monitoraggio e allarmistica) dal sistema di management eSight (Tipo 10) incluso all'interno della Convenzione.

4.5.2. Fortinet FG-3100D-BDL-C

L'apparato proposto come dispositivo per la sicurezza di fascia enterprise è il FortiGate 3100D, che è un appliance di fascia large Enterprise / Big Data Center.

La serie FortiGate 3100D offre funzionalità di firewall di nuova generazione (NGFW) ad alte prestazioni per grandi aziende e service provider che necessitano di elevate prestazioni di firewalling e IPS. Con più tipologie di interfacce ad alta velocità, alta densità di porte e throughput elevato, è l'apparato ideale per gestire applicazioni aziendali e di core data center ibrido. Il FortiGate 3100D sfrutta le funzionalità IPS di livello high end, la SSL inspection e protezione avanzata dalle minacce per ottimizzare le prestazioni della rete. L'approccio di Fortinet Security-Driven Networking fornisce una stretta integrazione tra rete e nuova generazione di sicurezza, che richiede ispezione del traffico senza compromessi di performance

Di seguito sono riportati i requisiti minimi e migliorativi richiesti nella gara per i dispositivi di fascia enterprise.

Requisiti minimi per i dispositivi di sicurezza di fascia enterprise:

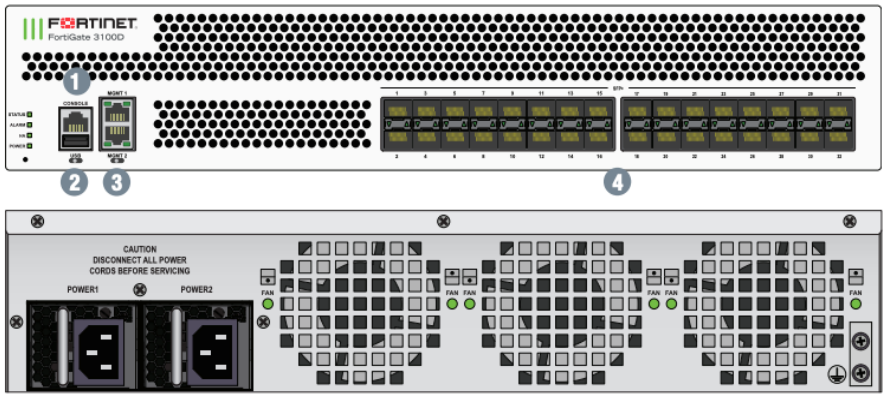
- Funzionalità Antivirus
- Funzionalità di Application Control
- Funzionalità di Intrusion Prevention System (IPS)
- Funzionalità Firewall
- VPN IPSec
- Funzionalità web/url filtering
- Almeno 10 interfacce 1000Base-T
- Almeno 4 interfacce Gigabit Ethernet SFP o SFP+ - esclusi i transceiver
- Almeno 4 interfacce 10 Gigabit Ethernet SFP+ - esclusi i transceiver
- Intrusion Prevention throughput almeno pari a 15 Gbps
- Firewall throughput almeno pari a 40 Gbps
- VPN throughput almeno pari a 12 Gbps
- Almeno 20 milioni di sessioni contemporanee
- Almeno 200.000 nuove sessioni al secondo

Caratteristiche migliorative per i dispositivi di sicurezza di fascia enterprise:

- Funzionalità antispam
- Meccanismi di rilevazione e protezione per attacchi di tipo Denial of Service
- Almeno 2 ulteriori interfacce Gigabit Ethernet SFP o SFP+ - esclusi i transceiver
- Almeno 4 ulteriori interfacce 10 Gigabit Ethernet SFP+ - esclusi i transceiver
- Funzionalità di TLS o SSL Inspection
- Supporto per configurazioni High Availability
- Funzionalità VPN TLS o SSL
- Supporto IPv6
- Funzionalità di traffic shaping (gestione QoS)
- Presenza di almeno 10 contesti virtuali

- Miglioramento di almeno il 30% delle prestazioni minime previste per l'Intrusion Prevention throughput (19,5 Gbps)
- Miglioramento di almeno il 30% delle prestazioni minime previste per Firewall throughput (52 Gbps)
- Miglioramento di almeno il 30% delle prestazioni minime previste per VPN throughput (15,6 Gbps)
- Miglioramento di almeno il 30% delle prestazioni minime previste per il numero di sessioni contemporanee (26 M)
- Miglioramento di almeno il 30% delle prestazioni minime previste per il numero di nuove sessioni al secondo (260.000)

Il Fortigate 3100D è un appliance di fascia large enterprise/big DC che soddisfa tutti i suddetti requisiti, sia minimi che migliorativi.



Interfaces

1. Console Port
2. USB Management Port
3. 2x GE RJ45 Management Ports
4. 32x 10G SFP+/GE SFP Slots

Questo dispositivo è dotato di 32 interfacce SFP/SFP+ corredato da 8 tranceiver 1000base-T per soddisfatre il requisito relativo al numero di porte rame richieste. Il sistema viene offerto completo di subscription Fortiguard UTP (Unified Threat Protection) per i servizi di Application Control, IPS, AV (AntiMalware Protection), Web Filtering ed Antispam.

Il FortiGate 3100D dispone del sistema operativo FortiOS comune a tutte le piattaforme di firewall Fortinet. Il sistema operativo FortiOS fornisce all'utente un elevato numero di funzionalità aggiuntive incluse nell'offerta senza necessità di ulteriori subscription. In particolare, all'interno del pacchetto base sono presenti tutte le funzionalità necessarie all'implementazione semplice e sicura di architetture SD-WAN. L'implementazione Secure SD-WAN del FortiOS garantisce un controllo intelligente dei percorsi su rete WAN, con o senza overlay IP-SEC, utilizzando più di 3000 applicazioni o utenti/gruppi per gestire le metriche di qualità della rete ed implementando politiche di routing e bandwidth management con l'utilizzo delle funzionalità di Quality of Service e Traffic Shaping.

Il livello di subscription fornito garantisce l'accesso anche alle seguenti funzionalità:

- Funzionalità FortiOS
    - SSL Inspection
    - SD-WAN
    - Routing e NAT con supporto per la Traffic Redirection con ICAP (Internet Content Adaptation Protocol)
    - L2 Switching (con supporto VXLAN e EMAC)
    - Explicit Proxy
    - Quality of Service (QoS) e Traffic Shaping
    - Data leak prevention (DLP)
    - Controller integrato per FortiSwitch e FortiWiFi
- FortiCare; include Internet Service DB, Client ID DB, IP Geography DB, Malicious URL DB, URL Whitelist DB
- Advanced Malware Protection (AMP)
    - Mobile Malware Security; per proteggere i client dalle minacce destinate a device mobili. La subscription include le funzionalità di mobile application control e protezione antimalware per piattaforme Apple IOS ed Android
    - Botnet
    - Content Disarm and Reconstruction (CDR); per rimuovere gli allegati malevoli e sostituirli con un file "disarmato"
    - Virus Outbreak Protection; servizio di verifica delle firme antivirus in tempo reale.
- DNS Filtering: il servizio permette di filtrare direttamente le query DNS per evitare traffico http verso domini compromessi
- FortiSandbox Cloud Service; servizio che permette di massimizzare la protezione dalle minacce 0-day e identificare un attacco sulla base di tecniche di analisi avanzata e sandboxing. Il servizio, richiesto in gara è già disponibile nel bundle dei servizi e non è soggetto a costi aggiuntivi

La tabella seguente fornisce un dettaglio delle specifiche tecniche e prestazionali della macchina:

Specifiche hardware	
Interfacce SFP/SFP+ complessive	32
Interfacce di management	2

Porte Console (RJ45)	1
Porte USB	1
Performance di Sistema	
Firewall Throughput (1518 / 512 / 64 byte, UDP)	80 / 80 / 50 Gbps
IPv6 Firewall Throughput (1518 / 512 / 64 byte, UDP)	80 / 80 / 50 Gbps
Latenza Firewall (64 byte UDP packets)	3 µs
Firewall Throughput (Pacchetti per Secondo)	75 Mpps
Sessioni Concorrenti (TCP)	50 Million
Nuove Sessioni/Secondo (TCP)	400.000
Firewall Policies	200.000
IPsec VPN Throughput (512 byte)	50 Gbps
Gateway-to-Gateway IPsec VPN Tunnels	40.000
Client-to-Gateway IPsec VPN Tunnels	200.000
IPS Throughput (Enterprise Traffic Mix)	22 Gbps
SSL-VPN Throughput	8 Gbps
SSL Inspection Throughput (IPS, HTTP)	16 Gbps
Application Control Throughput (HTTP 64K)	40 Gbps

CAPWAP Throughput (1444 byte, UDP)	22 Gbps
Virtual Domains (Default / Max supportati)	10/500
Numero Massimo di FortiSwitches Supportati	256
Numero Massimo di FortiAPs (Totali / Tunnel Mode)	4096 / 2048
Numero Massimo di FortiTokens	20.000
Configurazioni di High Availability	Active/Active, Active/Passive, Clustering
Dimensioni	
Altezza x Larghezza x Lunghezza (mm)	88 x 442 x 555
Peso	17.1 kg
Form Factor	2 RU
Secondo Alimentatore per ridondanza 2N, interno Hot-Swappable	incluso

Riferimenti documentali pubblici:
https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_3100D.pdf

4.5.3. Checkpoint CPAP-SG23500-NGTP-HPP

In fase di sostituzione per End of Sale

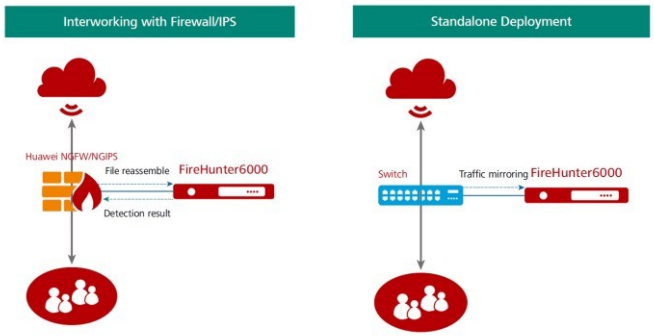
4.6. Dispositivi di sicurezza sandbox

4.6.1. Huawei FireHunter6300

Utilizzando la scansione basata su virus engine dei migliori vendor di soluzioni Antivirus nell'industria e meccanismi di reputazione, l'analisi statica e le tecnologie di esecuzione virtuale così come la libreria di modelli

di comportamento unica di Huawei, il FireHunter6000 è in grado di rilevare file dannosi non conosciuti e fornire rapporti di rilevamento accurati di conseguenza.

Interagisce con i dispositivi di sicurezza HiSecEngine Next Generation Firewall 6500E/6600E per bloccare rapidamente i file dannosi avanzati, impedendo minacce sconosciute di diffondere e proteggere le risorse di informazioni fondamentali per le imprese.



È un appliance 2 Rack Unit, doppia alimentazione con 8 interfacce GE e 2 interfacce 10GE e può essere dispiegato in modalità standalone o in cluster.

Huawei FireHunter6000 series sandbox

4.6.2. Fortinet FSA-1000F-BDL-C

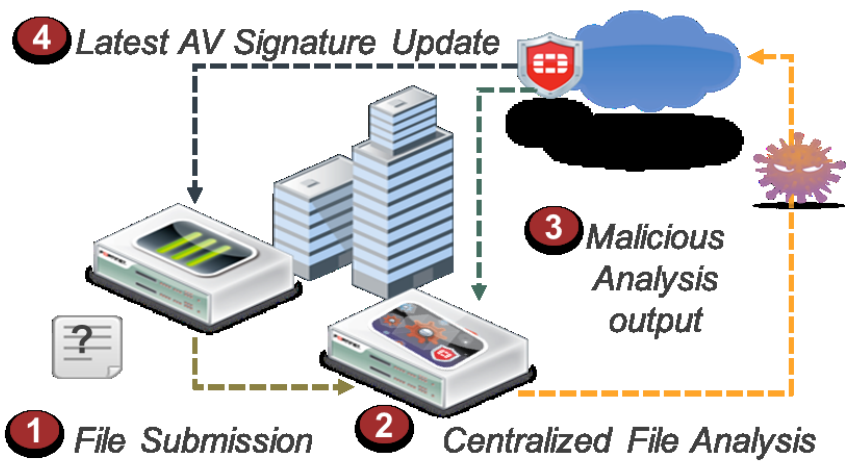
Fortisandbox è la soluzione progettata da Fortinet per la rilevazione di tipologie di attacchi informatici altamente mirati e confezionati ad hoc, che si annidano nelle reti e vengono ignorati dalle difese tradizionali. In genere questi attacchi sono noti con il nome di APT (Advanced Persistent Threat) e per contrastarli è necessario un approccio multilivello: Fortisandbox offre la più recente tecnologia e impiega una combinazione di mitigazione proattiva, visibilità avanzata delle minacce e reporting completo; si avvale delle tecnologie Fortinet di scansione antimalware, sandboxing a due livelli (lightweight e full) e cloud query ai Fortiguard Labs per individuare le tecniche di evasione e avere una protezione dalle minacce allo stato dell'arte. Le tecniche di

analisi avanzata di Fortinet si basano sul brevetto CPRL (Compact Pattern Recognition Language) che permette di rilevare con un singolo signature decine di migliaia di variazioni del codice virale e su algoritmi di Machine Learning e Intelligenza Artificiale che intervengono sia nell'analisi statica che nell'analisi dinamica.

FortiSandbox offre una protezione altamente efficace contro questa classe emergente di minacce oltre ad avere una notevole flessibilità di deployment e semplicità di gestione.

Le caratteristiche principali del FortiSandbox includono:

- Motore Antimalware dinamico e aggiornamenti/query verso il cloud Fortinet: gli aggiornamenti vengono effettuati dai FortiGuard Labs, a cui può inviare query in tempo reale, permettendo così di rilevare in modo veloce minacce esistenti ed emergenti.
- Emulazione di Codice: esegue in tempo reale una ispezione di tipo "lightweight sanboxing", in cui riescono ad identificare tipologie di malware che utilizzano tecniche di evasione e/o si attivano solo in presenza di versioni software specifiche. In questa fase viene implementato anche un algoritmo di Machine Learning per ottenere un rating più preciso
- Ambiente virtuale completo (detonazione): fornisce un ambiente isolato per analizzare codice sospetto o ad alto rischio, permettendo di esplorare e verificare l'intero ciclo di vita della minaccia. I tracer log relativi alla detonazione alimentano un algoritmo di intelligenza artificiale che contribuisce alla identificazione delle minacce più avanzate
- Visibilità avanzata: fornisce un quadro globale in una vasta gamma di reti, sistemi e attività di file classificati per livello di rischio, per migliorare la velocità di risposta agli incidenti.
- Network Alert: controlla il traffico di rete e rileva le richieste verso siti "malicious", che stabiliscono comunicazioni con server C&C e altre attività che sono indice di compromissione della sicurezza.
- Analisi Manuale: consente agli amministratori di sottomettere manualmente campioni di malware per effettuare sandboxing virtuale senza la necessità di avere un dispositivo separato.
- Submission al FortiGuard (opzionale): i tracer report, i file malicious e altre informazioni possono essere sottomesse ai FortiGuard Labs per ricevere raccomandazioni di bonifica e protezioni in linea aggiornate.



La soluzione Fortisandbox è molto flessibile, offrendo diversi scenari di deployment che permettono di adattarsi alle esigenze e ai requisiti dei clienti.

Essa prevede principalmente tre metodi di input con cui può esaminare il traffico di rete ed analizzare i file:

- On demand

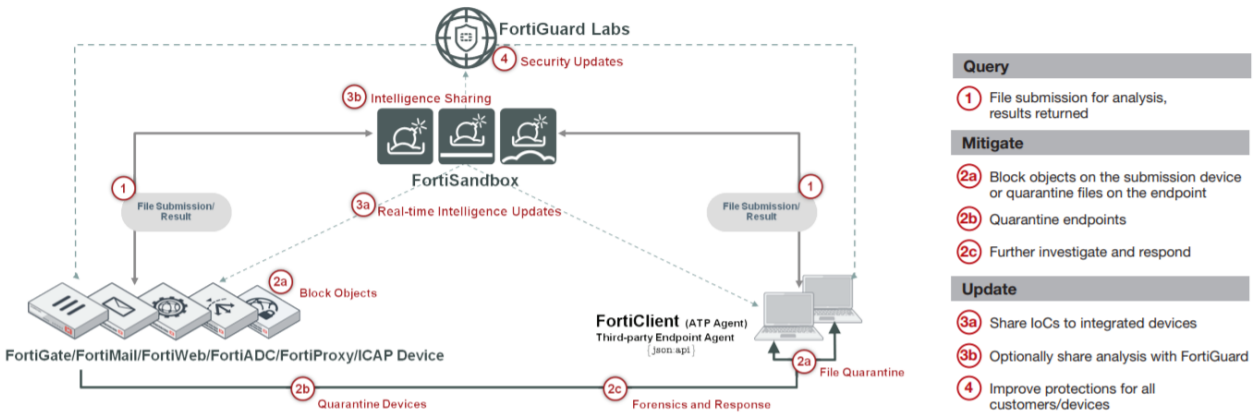
In questa modalità gli amministratori possono sottomettere manualmente campioni di malware per effettuare attività di analisi in sandboxing e verificarne i risultati in un ambiente isolato.

- Sniffer Mode

In questa modalità Fortisandbox riceve il traffico che viene spillato da porte in SPAN di switch di rete o utilizzando TAP: è in grado di analizzare i protocolli HTTP, FTP, POP3, IMAP, SMTP e numerose estensioni di files.

- Device Mode

Soluzioni Fortinet, quali FortiGate, FortiMail, FortiWeb, FortiClient (ATP Agent), FortiADC e fornitori di sicurezza di terze parti (tramite API e ICAP) possono intercettare e inviare i contenuti sospetti al FortiSandbox che effettuerà una serie di analisi volte a rilevare malware di tipo zero-day e APT. L'integrazione fornirà anche tempestive capacità di alert, remediation e reporting che sono caratteristiche della soluzione offerta.



In particolare, l'integrazione con il FortiGate permette anche l'analisi dei protocolli supportati con crittografia ssl, utilizzando le funzionalità di SSL deep inspection.

Le tre modalità di input possono essere attivate contemporaneamente su interfacce diverse dell'appliance.

Di seguito sono riportati i requisiti minimi e migliorativi richiesti nella gara per i dispositivi sandbox di tipo appliance:

Requisiti minimi per i dispositivi Sandbox:

- Supporto di almeno le seguenti tipologie di file: .zip, .gz, .bz2, .exe, .dll, .bat, .pdf, .jar, .doc, .docx, .xls, .xlsx, .ppt, .pptx, .mp4, .jpeg, .gif, .png
- Supporto di almeno i seguenti protocolli/applicazioni: HTTP, SMTP
- Scansione di almeno 100 files/ora
- Supporto di almeno 4 macchine virtuali
- Storage interno almeno 1 TB

- Almeno 2 interfacce 10/100/1000Base-T

Caratteristiche migliorative per i dispositivi Sandbox:

- Power supply ridondata
- Supporto di ulteriori tipologie di file rispetto alle minime richieste: - 2 ulteriori tipologieoppure- almeno 3 ulteriori tipologie
- Supporto di almeno 2 ulteriori protocolli/applicazioni rispetto ai minimi richiesti
- Almeno 2 ulteriori interfacce Gigabit Ethernet SFP o SFP+ - esclusi i transceiver
- Supporto di almeno 8 macchine virtuali
- Scansione di almeno 200 files/ora
- Supporto IPv6
- Almeno 2 ulteriori interfacce 10/100/1000Base-T
- Dello stesso brand dei Next Generation Firewall

La FortiSandobx 1000F (2 VM base) con una licenza aggiuntiva di 6 VM e un alimentatore per ridondanza, è un appliance sandbox che soddisfa tutti i suddetti requisiti, sia minimi che migliorativi.

In questa configurazione con 8 VM, si può ottenere un throughput di 160 Files/ora in caso di full sandboxing (caso peggiore) e circa 4000 file/ora in caso di real-word effective throughput (combinazione di analisi statica, machine learning, full sandboxing con Intelligenza Artificiale).

① 4x GE RJ45 Ports
② 4x GE SFP Slots
③ 2x 1TB Storage
④ Optional Redundant Power Supply

L'appliance è dotata di 4 interfacce rame RJ45 e 4 slot GE SFP, 2 hard disk da 1TB con possibile configurazione RAID; supporta fino a 14 VM (con ulteriore licenza aggiuntiva) ed un VM Sandboxing Throughput di 280 Files/ora in caso di full sandboxing, 7500 file/ora in caso di real-word effective throughput.

	FSA-1000F/-DC
Hardware	
Network Interfaces	4x GE RJ45 ports, 4x GE SFP slots
Storage	2x 1 TB
Power Supplies	1x PSU, Optional 2nd PSU for hot-swap
System Performance and Capacity	
Number of VMs	14*
Sandbox Pre-Filter Throughput (Files/Hour)[1]	7,500
VM Sandboxing Throughput (Files/Hour)	280
Real-world Effective Throughput (Files/Hour)	1,400[2]
Sniffer Throughput	1 Gbps
MTA Capacity	10,000 emails/hour
Dimensions and Power	
Height x Width x Length (inches)	1.73 x 17.24 x 22.83
Height x Width x Length (mm)	44 x 438 x 580
Weight	25 lbs (11.34 kg)
Form Factor	1 RU
Power Supply (AC/DC)	100–240V AC, 50/60 Hz / -48VDC
Maximum Current (AC/DC)	100V/5A, 240V/3A / -48VDC/9A
Power Consumption (Average/Maximum)	66.93 / 116.58 W
Heat Dissipation	397.75 BTU/h
Environment	
Operation Temperature Range	32–104°F (0–40°C)
Storage Temperature Range	-40–158°F (-40–70°C)
Humidity	5–90% non-condensing
Compliance	
Certifications	FCC Part 15 Class A, RCM, VCCI, CE, BSMI, KC, UL/cUL, CB, GOST

Riferimenti documentali pubblici:

https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiSandbox.pdf

4.7. Network Access Control

4.7.1. HPE JZ508A

Aruba ClearPass Policy Manager offre a dipendenti, collaboratori e ospiti, il controllo di accesso alla rete, basato sui ruoli e sui dispositivi, su infrastrutture cablate, wireless o VPN multi-vendor. Dotato di un motore di policy basato su RADIUS, supporto del protocollo TACACS+, creazione di profili per i dispositivi e valutazione del loro stato, onboarding e opzioni di accesso guest, Aruba ClearPass non ha rivali per ciò che riguarda la sicurezza della rete.

Aruba ClearPass Policy Manager supporta funzionalità di tipo "self-service", facilitando l'accesso in rete per gli utenti finali; questi ultimi possono infatti configurare i propri dispositivi per l'uso aziendale o l'accesso a Internet, in base alle policy configurate. Un altro vantaggio offerto dalla soluzione è che gli utenti che possiedono un'infrastruttura Wi-Fi Aruba possono condividere proiettori, TV, stampanti e altre appliance multimediali che utilizzano DLNA/UPnP o Apple AirPlay e AirPrint; ClearPass semplifica infatti l'individuazione di tali dispositivi e la condivisione tra gli utenti.

Questa piattaforma di gestione delle policy, completa e scalabile, va quindi oltre le tradizionali soluzioni di autenticazione, autorizzazione e accounting (AAA), per offrire funzionalità di enforcement che rispondono ai requisiti di sicurezza richiesti per esempio per il Bring-Your-Own-Device (BYOD).

Con le policy di ClearPass e la soluzione AAA integrata si può usufruire della creazione di profili, di un'interfaccia amministrativa basata sul Web e funzionalità complete di reporting con avvisi in tempo reale. Tutti i dati contestuali raccolti vengono sfruttati per garantire che a tutti gli utenti e i dispositivi vengano concessi privilegi di accesso appropriati, indipendentemente dal metodo di accesso o dalla proprietà del dispositivo.

Un approccio all'applicazione delle policy basato su template offre all'IT la possibilità di creare policy orientate sia alle reti cablate che alle reti wireless che sfruttino elementi come ruoli dell'utente, tipi di dispositivi, dati MDM/EMM, stato dei certificati, posizione, giorno della settimana e altro ancora. Le policy possono quindi facilmente applicare regole per dipendenti, studenti, medici, utenti guest, dirigenti e per ciascun tipo di dispositivo che tali utenti decidono di utilizzare.

Per maggiori Informazioni e per una documentazione esaustiva in merito ai prodotti e la guida utile alla configurazione, si rimanda al seguente link: Secure Your Network Architecture With HPE Aruba NAC

Licensing

Aruba ClearPass Policy Manager offerto in convenzione è equipaggiato con il **set completo di licenze**, in modalità **perpetua e senza alcuna necessità di rinnovo di licenze e rinnovo di subscription**. Il Policy manager proposto è quindi provvisto di tutte le funzionalità di cui dispone e senza alcun tipo di scadenza. Di seguito vengono dettagliate le funzionalità delle licenze.

ClearPass Onboard

ClearPass Onboard consente agli utenti di configurare in completa autonomia i dispositivi in modo da poterli utilizzare nelle reti protette. Grazie a certificati specifici per i dispositivi, gli utenti non devono più immettere le credenziali di accesso varie volte nell'arco di una giornata, e questa maggiore praticità rappresenta già di per sé un traguardo. Un ulteriore vantaggio è costituito dalla maggiore sicurezza garantita dall'uso dei certificati.

- CLEARPASS ONBOARD – Licenze perpetue e senza limitazioni di utilizzo

Accesso guest semplice e rapido

L'approccio BYOD non riguarda solo i dispositivi dei dipendenti, bensì comprende qualsiasi visitatore con un dispositivo che richiede l'accesso alla rete, cablata o wireless.

Con ClearPass Guest i dipendenti, gli addetti alla reception, i coordinatori di eventi e altro personale non IT possono creare in modo semplice ed efficiente account temporanei per l'accesso alla rete, per un numero indefinito di guest ogni giorno. Il caching degli indirizzi MAC garantisce inoltre che gli utenti guest possano facilmente connettersi durante tutto l'arco della giornata senza dover immettere ripetutamente le credenziali nel portale guest.

Con l'auto-registrazione i dipendenti non devono più occuparsi di questa attività e gli utenti guest possono creare direttamente le proprie credenziali. Le credenziali di accesso vengono fornite tramite badge stampati, SMS o e-mail. Possono inoltre essere archiviate in ClearPass per determinati periodi di tempo, configurando una scadenza automatica dopo un certo numero di ore o giorni.

- ACCESSO GUEST – Licenze perpetue e senza limitazioni di utilizzo

ClearPass Onguard

Durante il processo di autorizzazione, può essere necessario svolgere delle valutazioni dello stato di specifici dispositivi, al fine di garantire che siano conformi ad alcune policy, come ad esempio dell'antivirus, dell'anti-spyware e del firewall. L'automazione può spingere gli utenti ad eseguire scansioni antivirus prima di connettersi alla rete aziendale.

ClearPass OnGuard è dotato di capacità integrate, che svolgono controlli dello stato dei dispositivi per eliminare vulnerabilità in un'ampia gamma di sistemi operativi e versioni di computer. Indipendentemente dal fatto che si utilizzino client permanenti o temporanei, ClearPass può identificare gli endpoint conformi ai requisiti in infrastrutture wireless, cablate e VPN.

- CLEARPASS ONGUARD – Licenze perpetue e senza limitazioni di utilizzo

Integrazione con terze parti

ClearPass consente di automatizzare la risposta alle eventuali minacce alla sicurezza e di migliorare i servizi utilizzando soluzioni di terze parti molto diffuse quali firewall, MDM/EMM, MFA, tool di registrazione dei visitatori e SIEM; ha quindi l'abilità di rispondere ad un eventuale attacco anche se questo viene segnalato da un Vendor di sicurezza.

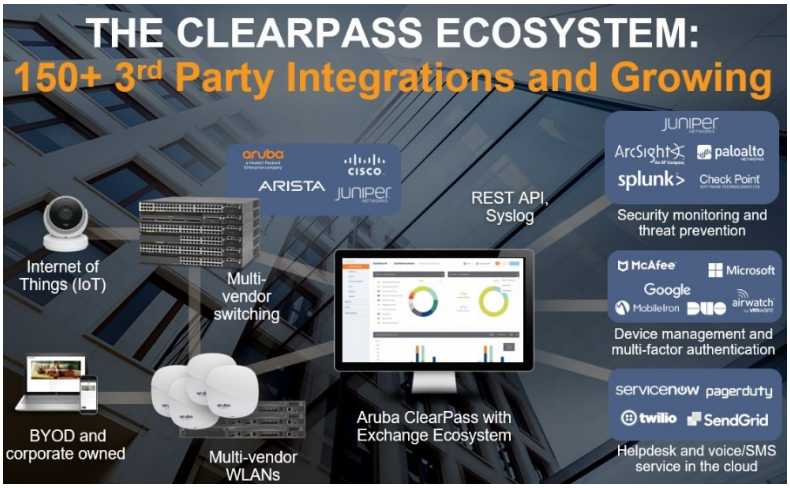
Workflow e processi decisionali automatizzati, che si avvalgono di REST API, messaggistica syslog e un repository integrato contribuiscono a semplificare le attività e rendere sicura l'azienda, senza ricorrere a complessi linguaggi per la creazione di script o lunghe configurazioni manuali.

Grazie a questo tipo di integrazioni le reti possono agire automaticamente:

- I dati MDM/EMM possono servire a determinare lo stato di un dispositivo e se quest'ultimo può connettersi alla rete.

- I firewall possono applicare le policy in modo accurato sulla base di attributi dell'utente, di gruppo e specifici del dispositivo, nonché usufruire di ClearPass per rimediare ad un comportamento inappropriato di un dispositivo.
- Gli strumenti SIEM possono essere configurati in modo da archiviare i dati di autenticazione per tutti i dispositivi connessi.
- Agli utenti può essere richiesto di utilizzare l'autenticazione MFA (Multi-Factor Authentication) per dimostrare la propria identità al momento della connessione alle reti e alle risorse.

Gli eventi di rete possono inoltre inviare prompt ai firewall, a SIEM e agli altri strumenti per indicare a ClearPass di intervenire in merito a un dispositivo attivando azioni in maniera bidirezionale. Se, ad esempio, un utente fallisce più volte nelll'autenticazione di rete, ClearPass può attivare un messaggio di notifica direttamente nel dispositivo oppure può inserirlo in una blacklist per impedire l'accesso alla rete.

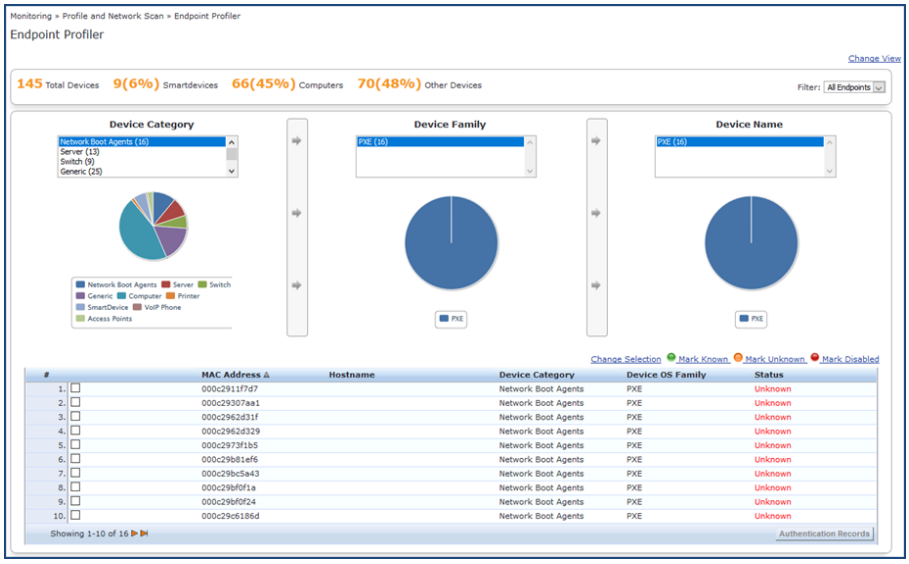


Visibilità degli endpoint connessi alle reti wired e wireless

Il requisito fondamentale per definire una politica di controllo degli accessi alla rete aziendale che sia chiara, corretta e sicura consiste nell'avere una dettagliata visibilità del numero dei dispositivi, della loro tipologia e necessità degli stessi.

A tal scopo, Clearpass contiene un modulo chiamato "Device Profiler" che automaticamente profila e classifica i dispositivi all'atto dell'accesso in rete, mediante una serie di componenti software chiamati "collectors" e un database di "fingerprints" costantemente aggiornato.

Le informazioni raccolte sono fruibili mediante grafici e tabelle, in maniera aggregata o visualizzando il dettaglio di un singolo dispositivo o di un sottogruppo



KEY FEATURES

La scelta di Aruba Clearpass, presente in Convenzione Consip Lan 7, permette al cliente di avere diversi vantaggi, che si basano sui numerosi punti di forza del prodotto.

Multi vendor

- ha la capacità di sviluppare, automatizzare, applicare e controllare policy di sicurezza all'accesso sia in reti Aruba, che di altri Vendor, supportando oltre 100 dizionari RADIUS e offrendo massima flessibilità all'utente finale;
- implementabile sia per reti cablate che wireless e applicabile a livello globale su molti settori di mercato.
- le soluzioni offerte da altri Vendor non forniscono visibilità e controllo centralizzati da un unico sistema integrato su reti eterogenee.

Interoperabilità

- ClearPass utilizza protocolli e interfacce basati su standard (ad es. Web API standard per ricevere dati da risorse esterne)
- La soluzione è integrata con centinaia di strumenti aziendali e applicazioni di uso comune (ad esempio firewall Palo Alto Networks, McAfee anti-malware)
- Offre connettività ad altri sistemi di gestione (ad es. MDM): Aruba lavora infatti con oltre 5 partner MDM (inclusi AirWatch, MobileIron e Citrix)
- Fornendo API e flessibilità, Clearpass può essere integrato e implementato in qualsiasi ambiente di qualsiasi Vendor e supportare la maggior parte dei dispositivi smart mobile.

Scalabilità

- Clearpass è in grado di gestire in maniera vincente la sicurezza di accesso alla rete in implementazioni su larga scala e l'autenticazione in alta densità
- Può applicare le policy su più siti, da una singola piattaforma centralizzata
- È possibile aggiungere facilmente nuovi utenti

Semplicità di deployment

- Grazie a dei task automatizzati, Clearpass ha la capacità di profilare e d'implementare l'onboarding dei dispositivi in maniera automatizzata, semplificando la configurazione dei dispositivi stessi e l'implementazione delle policy
- Tramite la simulazione delle policy, i Clienti possono provare eventuali modifiche ad una policy offline e testarne gli effetti, prima d'implementarle.

A differenza di altri Vendor, con le sole licenze Access sono incluse tutte le funzionalità di base a livello NAC:

- AAA
- 802.1x
- MAC-Authentication
- Web Based User Registration e Authentication (captive portal authentication)
- Multi-Factor Authentication (MFA)
- TACACS+ per Device Administration (per es. Router, Switch, Controller, Firewall, ecc)
- OnConnect
- System APIs
- 360 Security Exchange
- Standard endpoint visibility (anche conosciuta come device fingerprinting)
- Guest
- Profiling
- Integrazione con MDM
- Integrazione con terze parti

Questa lista di funzionalità integrate è un vantaggio della soluzione Aruba Clearpass, anche rispetto ad altri Vendor, che per attivare ad es. il profiling, TACACS+, l'integrazione con MDM e con terze parti richiedono licenze aggiuntive ad hoc.

Profilazione

Ha la funzionalità di fingerprint per ogni dispositivo che si connette in rete e utilizza quest'informazione per l'implementazione delle policy. Mettendo insieme quest'aspetto con le informazioni che vengono identificate durante il processo di autenticazione e autorizzazione, possono essere create delle policy granulari (ad es. che identifichino e separino le policy dedicate a dei computer di dominio rispetto a quelle dei tablet personali).

Completezza della soluzione

ClearPass offre in modo univoco un set completo di funzionalità per la gestione della sicurezza dell'accesso alla rete in un unico sistema integrato:

- Policy management
- Policy enforcement
- Funzionalità Guest
- Device profiling e onboarding
- Automation
- Tool di troubleshooting

I moduli opzionali includono la self-registration e l'advertising dei guest, l'onboarding dei device e la convalida dello stato di salute dei dispositivi

Clearpass è completo di strumenti integrati che permettono l'analisi di eventuali problematiche (es. diagnostica per il troubleshooting di eventuali autenticazioni fallite).

Integrazione con terze parti

ClearPass ha l'ecosistema più esteso di interoperabilità di terze parti di qualsiasi prodotto NAC. Dall'AAA di base ai servizi cloud, la soluzione può interagire con qualsiasi prodotto di rete, comunicazione o sicurezza sul mercato. L'uso di protocolli di comunicazione standard come RADIUS, HTTP e Syslog, assicura che ClearPass interagisca con i dispositivi e i software attualmente distribuiti nelle reti attuali, eliminando costosi aggiornamenti di infrastrutture o software.

TIPOLOGIA DI LICENZE COMPRESE NEL BUNDLE

- **Licenze Access**

Le licenze Access sono le licenze base del ClearPass Policy Manager; il consumo di queste licenze si basa sul numero di endpoint contemporaneamente autenticati/autorizzati e vengono fornite in modalità perpetua e quindi senza necessità di rinnovi e/o ulteriori subscription

Una sessione è considerata attiva quando un endpoint è autenticato/autorizzato e attivamente connesso alla rete. Per cui, quando un nuovo endpoint stabilisce una sessione, una licenza Access viene rimossa dal pool di quelle disponibili; quando invece l'endpoint interrompe la sessione, una licenza Access viene restituita al pool. I controlli di sessione vengono eseguiti ogni 15 minuti e, se non è possibile identificare la fine della sessione, la licenza verrà rimossa dal pool per un periodo di 24 ore dal momento in cui l'endpoint è stato autenticato/autorizzato e connesso alla rete.

- **Licenze OnBoard**

Le licenze OnBoard sono utilizzate per abilitare il provisioning automatico e la creazione di certificati di identità univoci per qualsiasi dispositivo Windows, macOS, iOS, Android, ChromeOS e Linux, tramite un portale self-guided. Il consumo di licenze OnBoard si basa su un modello di certificato attivo per utente.

Ad esempio, se un determinato utente ha quattro dispositivi con un certificato attivo ciascuno, è necessaria una sola licenza OnBoard; se nel tempo, tre dei quattro dispositivi vengono ritirati e i loro certificati associati vengono revocati, il quarto certificato del dispositivo attivo manterrà comunque la licenza OnBoard associata all'utente.

- **Licenze OnGuard**

Le licenze OnGuard sono utilizzate per eseguire valutazioni avanzate sullo stato di salute dell'endpoint su connessioni wireless, cablate e VPN, assicurando la conformità e le garanzie necessarie all'infrastruttura di rete, prima della connessione dei dispositivi. Il consumo delle licenze OnGuard si basa su un modello per endpoint.

Ad esempio, se deve essere installato un agente OnGuard su cinque endpoint entro un periodo di 24 ore, sono necessarie cinque licenze OnGuard.

Dispositivi di sicurezza nac - fascia base fino a 100 Endpoint concorrenti

HPE ARUBA – Codice Prodotto JZ508A-100C

Componenti hardware fornite con bundle 100 Endpoint:

- 100 Licenze Access (Licenze perpetue,set completo di funzionalità)
- 100 Licenze OnBoard (Licenze perpetue,set completo di funzionalità)
- 100 Licenze OnGuard (Licenze perpetue,set completo di funzionalità)
- 1 Aruba ClearPass C1000 S-1200 R4 HW Appliance

- L'appliance C1000 è un modello hardware basato su Unicom S-1200 R4, con CPU Atom 2.40GHz C2758 con 8 Core (8 Threads), 8 GB di memoria, uno storage SATA (7.2K RPM) 1TB e supporta fino a 1000 sessioni concorrenti.

Dispositivi di sicurezza nac - fascia media fino a 500 Endpoint concorrenti

HPE ARUBA – Codice Prodotto JZ508A-500C

Componenti hardware fornite con bundle 500 Endpoint:

- 500 Licenze Access (Licenze perpetue,set completo di funzionalità)
- 500 Licenze OnBoard (Licenze perpetue,set completo di funzionalità)
- 500 Licenze OnGuard (Licenze perpetue,set completo di funzionalità)
- 1 Aruba ClearPass C1000 S-1200 R4 HW Appliance
    - L'appliance C1000 è un modello hardware basato su Unicom S-1200 R4, con CPU Atom 2.40GHz C2758 con 8 Core (8 Threads), 8 GB di memoria, uno storage SATA (7.2K RPM) 1TB e supporta fino a 1000 sessioni concorrenti.

Dispositivi di sicurezza nac - fascia alta fino a 1000 Endpoint concorrenti

HPE ARUBA – Codice Prodotto JZ508A-1000C

Componenti hardware fornite con bundle 1000 Endpoint:

- 1000 Licenze Access (Licenze perpetue,set completo di funzionalità)
- 1000 Licenze OnBoard (Licenze perpetue,set completo di funzionalità)
- 1000 Licenze OnGuard (Licenze perpetue,set completo di funzionalità)

- Aruba ClearPass C1000 S-1200 R4 HW Appliance
    - L'appliance C1000 è un modello hardware basato su Unicom S-1200 R4, con CPU Atom 2.40GHz C2758 con 8 Core (8 Threads), 8 GB di memoria, uno storage SATA (7.2K RPM) 1TB e supporta fino a 1000 sessioni concorrenti.

Dispositivi di sicurezza nac - fascia top fino a 10000 Endpoint concorrenti

HPE ARUBA – Codice Prodotto JZ509A-10000C

In fase di sostituzione per End of Sale

Dispositivi di sicurezza nac - fascia top macchina virtuale fino a 10000 Endpoint concorrenti

HPE ARUBA – Codice Prodotto JZ399AAE-10000C

Componenti hardware fornite con bundle 10000 Endpoint:

- 10000 Licenze Access (Licenze perpetue,set completo di funzionalità)
- 10000 Licenze OnBoard (Licenze perpetue,set completo di funzionalità)
- 10000 Licenze OnGuard (Licenze perpetue,set completo di funzionalità)
- Aruba ClearPass Cx000V VM Appliance E-LTU
    - Le appliance virtuali richiedono specifiche di risorse simili a quelle presenti nei prodotti hardware, in modo da garantire un'esperienza ClearPass coerente indipendentemente dall'hardware o dall'appliance virtuale.

Clearpass Policy Manager è supportato attualmente dai seguenti hypervisor e virtual private cloud:

- VMware vSphere Hypervisor (ESXi) 6.0, 6.5, 6.5 U1, 6.5 U2, 6.7, 6.7 U1, and 6.7 U2
- Microsoft Hyper-V Server 2012 R2, Microsoft Hyper-V Server 2016, Microsoft Hyper-V Server 2019, Windows Server 2012 R2 with Hyper-V, or Windows Server 2016 with Hyper-V
- KVM on CentOS 7.5
- Amazon Web Services

Per maggiori Informazioni e per una documentazione esaustiva in merito ai prodotti e la guida utile alla configurazione, si rimanda al seguente link: Secure Your Network Architecture With HPE Aruba NAC.

4.7.2. Forescout

Forescout Technologies è il leader riconosciuto della sicurezza per l'Enterprise of Things, ossia per tutti i dispositivi, di qualunque genere essi siano, che insistono e si connettono a qualunque tipo di infrastruttura di rete presente all'interno di una azienda/organizzazione.

Forescout Technologies è in grado di offrire l'unica soluzione scalabile che difende attivamente l'Enterprise of Things identificando, segmentando e imponendo la conformità di ogni dispositivo connesso alla rete eterogenea del cliente.

Forescout Technologies è in grado di fornire la possibilità di integrare la propria piattaforma con una vasta pletora di tecnologie di sicurezza già in uso presso il Cliente al fine di incrementare il livello di sicurezza ed il valore complessivo degli investimenti fatti nell'ambito della sicurezza informatica.

La piattaforma NAC di Forescout Technologies viene distribuita in modo rapido nell'infrastruttura esistente senza richiedere necessariamente l'installazione di agent, l'aggiornamento dei sistemi né modifiche sostanziali alla infrastruttura di rete del cliente.

Forescout Technologies da oltre venti anni non ha mai venduto un semplice prodotto ma ha sempre venduto il successo e la soddisfazione dei Clienti, come ampiamente confermato sia dalle referenze dei clienti che dagli innumerevoli riconoscimenti che la propria tecnologia ha ricevuto nei più disparati ambiti.

Visibilità e controllo dei dispositivi: Perché non puoi farne a meno

La capacità di individuare, classificare, valutare e controllare ogni dispositivo connesso alla propria rete è un presupposto essenziale per conseguire una sicurezza informatica di tipo Zero Trust.

Solo chi possiede una conoscenza in tempo reale degli endpoint (sia fisici che virtuali) presenti in ogni segmento di rete, chi ha le informazioni dettagliate sul livello e sullo stato di sicurezza degli stessi, e chi ha funzionalità automatizzate di controllo degli accessi e di remediation basate su policy predefinite, può essere certo che i sistemi e i dati siano protetti, avendo la possibilità di reagire rapidamente e con precisione agli eventuali problemi di sicurezza informatica.

I criminali informatici sono costantemente alla ricerca di dispositivi non gestiti e non protetti e non tarderanno a individuare i punti ciechi della rete e ad approfittarne. La visibilità dell'intera infrastruttura e il controllo della stessa in modalità Agentless sono i pilastri su cui si basano la sicurezza e la conformità. Queste capacità giocano inoltre un ruolo essenziale nell'affrontare numerose problematiche di sicurezza informatica all'interno dell'azienda.

La visibilità in tempo reale, in modalità h.24, e legata al contesto operativo dei vari endpoint connessi sull'intera infrastruttura di rete (comprensiva cioè dell'area Campus, dell'area Data Center e dell'area Cloud) permette di ottenere un accurato inventario delle risorse in tempo reale (Asset Management) in grado di ridurre i costi operativi legati al personale presente nei NOC (Network Operation Center) e nei SOC (Security Operation Center), assicurando contemporaneamente il rispetto della conformità alle varie normative (sia aziendali, che di settore e/o comunitarie) ed evitando in tal modo il mancato superamento delle attività di revisione (e delle possibili conseguenze in termini legali/economici).

Perché la visibilità e il controllo sono così difficili da ottenere

Il metodo tradizionale a cui si ricorreva per gestire gli endpoint della rete consisteva nell'installare un software su ogni dispositivo. Questo metodo funzionava quando la maggior parte degli endpoint era statica, costituita da PC o server di proprietà dell'azienda. La mobilità, la diversità dei tipi di dispositivo e la virtualizzazione hanno reso la visibilità contestualizzata e il controllo della infrastruttura molto più complicati.

L'esplosione nel numero e nella diversità dei dispositivi ha radicalmente alterato il panorama stesso degli endpoint installati sulle varie infrastrutture di rete. Nelle infrastrutture di rete sta esplodendo il livello di connettività dovuto agli apparati classificati come IoT (Internet of Things) e come OT (Operating Technologies) che prima operavano su reti fisicamente separate e che ora invece insistono sulla rete IT aziendale. Molte aziende/organizzazioni (anche a causa della pandemia Covid-19) hanno attuato un modello di lavoro sempre più basato su connessione dei propri dipendenti da remoto (Smart Working e/o Lavoro Agile). L'impresa moderna si è rapidamente evoluta nella "Enterprise of Things" e molti degli endpoint connessi sulla infrastruttura di rete non sono in grado di supportare gli agent di gestione.

Anche per quegli endpoint in grado di supportare un agent on-board l'approccio basato sugli agent è problematico. Infatti, i sistemi basati su agent non funzionano se l'agent manca, non funziona o è disattivato, i metodi basati su agent e sull'uso del protocollo IEEE 802.1X creano dei punti ciechi nella rete e introducono una estrema complessità operativa, con il risultato che spesso si realizzano distribuzioni incomplete.

Se isolati, gli strumenti per gestire la conformità dei dispositivi alle policy definite non godono di una visuale unificata, mantenendo in vita, così, i punti ciechi (blind-spot) all'interno dell'intera infrastruttura.

In molte reti il numero di dispositivi non gestiti supera abbondantemente il numero di quelli gestiti, e si tratta, di solito, di sistemi che non possono essere autenticati con metodi tradizionali.

I dipendenti mobili, coloro che utilizzano dispositivi BYOD, gli ospiti e gli utenti che fanno uso del telelavoro rendono la sicurezza dipendente dagli agent molto dispendiosa in termini di tempo, oltre che inefficace.

Le reti in cui sono presenti sistemi di più vendor sono molto diffuse e richiedono alternative all'autenticazione degli stessi basata sul protocollo IEEE 802.1X, autenticazione che non deve richiedere degli upgrade hardware e/o software né dei dispositivi né, tantomeno, delle infrastrutture di rete stesse.

Forescout Technologies per una soluzione NAC di ultima generazione

Per affrontare le problematiche prevalenti negli odierni ambienti dinamici e diversificati, Forescout Technologies ha introdotto, sin dall'inizio della sua attività più che ventennale, la metodologia di controllo dell'accesso alla rete (NAC) in modalità Agentless.

La piattaforma Forescout offre una visione continua (h.24) e unificata su tutti i dispositivi di ambienti fisici (reti Campus sia Wired che Wireless), Data Center (sia fisici che virtuali), Cloud (pubblici e/o privati) e reti di tipo industriale (con prevalenza di tecnologie di tipo Operativo).

La piattaforma fornisce visibilità continua e granulare su:

- Dispositivi di rete degli ambienti fisici (reti Campus): laptop, tablet, smartphone, sistemi BYOD/ospiti e dispositivi IoT;
- Infrastrutture dei Data Center: macchine virtuali, hypervisor, server fisici e altri componenti virtuali e fisiche per le reti;
- Infrastrutture di cloud pubblici e privati: macchine virtuali AWS®, Microsoft® Azure® e VMware® (sia ESX che NSX);

- Sistemi di tipo IoMT, OT e di controllo industriale (ICS): dispositivi medicali, industriali e di automazione degli edifici;
- Infrastrutture di rete sia fisiche che software: switch, router, firewall, VPN, access point wireless e controller.

Forescout Technologies - Come funziona

La soluzione NAC di Forescout consente ai dipartimenti IT di:

- Scegliere fra oltre 20 tecniche attive e passive per il rilevamento dei dispositivi in modalità Agentless evitando la creazione di punti ciechi (blind-spot) all'interno dell'infrastruttura;
- Classificare automaticamente e accuratamente i dispositivi individuati in base alla funzione, al sistema operativo (e relativa versione), alla marca e al modello;
- Creare e mantenere automaticamente ed in tempo reale, per ogni dispositivo connesso alla rete IP aziendale, un inventario delle risorse;
- Valutare e controllare continuamente lo stato di sicurezza di tutti i dispositivi, in modalità agentless;
- Conformarsi alle policy di sicurezza e alle normative di settore grazie alla possibilità di automatizzare la fase di ripristino degli endpoint sotto controllo;
- Imporre controlli flessibili della rete in base all'autenticazione, al ruolo degli utenti, al tipo dei dispositivi e allo stato di sicurezza individuato, in qualsiasi rete eterogenea (sia in modalità cablata, che in modalità wireless che in modalità VPN);
- Imporre il controllo degli accessi con privilegi minimi per la protezione Zero Trust.

Identificazione di ogni dispositivo su tutte le reti

La piattaforma NAC di Forescout utilizza oltre 20 tecniche (configurabili dall'utente) di raccolta dei dati.

Tali tecniche sfruttano l'integrazione profonda tra la piattaforma Forescout con la maggior parte dei vendor (oltre 40) produttori di switch per reti IT e OT, router, access point wireless, firewall, concentratori VPN e fornitori di soluzioni per data center e cloud.

La piattaforma ascolta, in modalità passiva, il traffico della rete analizzando i flussi di molteplici protocolli diversi ed è in grado di interagire con l'infrastruttura di rete e con gli endpoint per fornire una risposta quanto più veloce possibile ad eventuali problemi di sicurezza riscontrati.

Le tecniche di visibilità di Forescout includono:

- Metodi **passivi per la rete e per i dispositivi finali**: Rientrano in questa categoria la ricezione di trap SNMP da switch e controller wireless, il monitoraggio di porte SPAN e l'analisi di flussi di dati codificati con protocolli diversi (la piattaforma Forescout consente un esame approfondito dei pacchetti creati con più di 150 protocolli del mondo IT e del mondo OT), la raccolta e l'analisi dei dati di flusso, la valutazione delle richieste DHCP e l'analisi del traffico agente-utente di tipo HTTP. Nel caso in cui venga implementato lo standard 802.1X (che la piattaforma Forescout è in grado di gestire in modalità completa), la piattaforma Forescout monitora anche le richieste RADIUS utilizzando un server integrato oppure facendo uso di un eventuale server esterno preesistente;
- Metodi **attivi nell'infrastruttura di rete**: Rientrano in questa categoria il polling degli switch, dei concentratori VPN, dei controller wireless e dei controller per cloud privati e pubblici al fine di compilare l'elenco dei dispositivi connessi e delle macchine virtuali esistenti. Per ottenere i dati relativi agli utenti e agli endpoint, la piattaforma Forescout è in grado di interrogare i servizi di directory, le applicazioni web e i database esterni;
- Metodi **attivi nei dispositivi finali:** La piattaforma è in grado di effettuare la scansione dei segmenti di rete alla ricerca di dispositivi connessi utilizzando Nmap, è in grado di effettuare una ispezione remota di dispositivi Windows attraverso WMI o di dispositivi Mac e Linux utilizzando SSH, ed è in grado di eseguire la profilazione degli endpoint tramite query SNMP dirette agli endpoint stessi.

Il vantaggio di disporre di più metodi di individuazione

La piattaforma NAC di Forescout presenta un livello di efficienza, flessibilità ed efficacia unico perché mette a disposizione diversi metodi di individuazione degli endpoint che sono facilmente configurabili all'inizio e altrettanto facilmente modificabili in seguito.

- **Distribuzione semplificata e a costi contenuti in ambienti di grandi dimensioni:** La capacità di scegliere fra oltre 20 tecniche attive e passive offre la flessibilità necessaria per ottenere una visibilità completa sui dispositivi in qualsiasi rete eterogenea, a prescindere dalla sua complessità e dalle dimensioni o numero delle ubicazioni remote. Il tutto, senza dover effettuare l'upgrade dell'infrastruttura (software/hardware) né impiegare una appliance locale in ogni sito e/o ufficio remoto;
- **Nessun punto cieco (blind-spot):** non è insolito che le varie aziende/organizzazioni possiedano delle sedi remote dove non possono essere impiegate delle appliance aggiuntive né fornire il traffico SPAN. La capacità della piattaforma NAC di Forescout di sfruttare diverse tecniche, sia attive che

passive, risolve qualsiasi limitazione della rete e fornisce il 100% di copertura dei dispositivi senza punti ciechi;

- **Tecniche di individuazione, classificazione e valutazione passive per le reti critiche della sanità e dell'industria (OT/ICS).** In molti casi le reti critiche sono ambienti che non si prestano ad attività di sondaggio e scansione attive perché il rischio potenziale di interrompere sistemi medici e/o di controllo dei processi è troppo elevato. La piattaforma NAC di Forescout fornisce visibilità sulle reti sanitarie critiche e sulle reti industriali (OT/ICS) tramite una combinazione di tecniche interamente passive, fra le quali il monitoraggio del traffico SPAN per l'ispezione approfondita dei pacchetti di oltre 150 protocolli specifici in ambito IT, sanità e OT. Ciò che distingue la soluzione NAC di Forescout è che, una volta identificati accuratamente i dispositivi, può, eventualmente, e selettivamente, applicare i metodi attivi su dispositivi specifici per una valutazione aggiuntiva senza rischiare l'interruzione delle attività;

Non solo visibilità, ma classificazione e valutazione

Grazie alla sua capacità intrinseca di combinare tecniche di profilazione attive e passive, la piattaforma NAC di Forescout non si limiterà semplicemente a identificare un dispositivo connesso in base all'indirizzo MAC o IP. Per classificazione si intende il processo di acquisizione e messa in relazione di diversi strati di dati contestualizzati con l'obiettivo di creare un profilo altamente dettagliato di ogni dispositivo. La valutazione è il processo che consiste nel raffrontare le proprietà del dispositivo rilevato con le policy di sicurezza definite per esercitare il controllo degli accessi e per formulare le decisioni di ripristino.

Classificazione automatica e intelligente

Per creare policy granulari è fondamentale conoscere il contesto completo in cui opera ogni dispositivo. Per decidere come proteggere e gestire al meglio ciascun dispositivo, è necessario conoscerne la finalità operativa. L'aumento del numero e della varietà di dispositivi rende pressoché impossibile acquisire manualmente dati sul contesto e, d'altro canto, la creazione di policy senza un contesto adeguato è alquanto rischiosa. La piattaforma NAC di Forescout classifica automaticamente i dispositivi tradizionali, IoT e OT con una tassonomia multidimensionale che identifica la funzione, il tipo, la marca e il modello di ogni dispositivo, oltre al sistema operativo e alla versione.

La piattaforma NAC di Forescout è in grado di classificare automaticamente:

- Oltre 575 differenti versioni dei sistemi operativi;
- Oltre 5700 diverse marche e modelli di prodotti;

- I dispositivi sanitari di oltre 400 importanti produttori di tecnologia medicale;
- Migliaia di dispositivi di controllo e automazione industriale utilizzati nei settori manifatturiero, energetico, petrolio e gas, servizi pubblici, minerario e altri settori delle infrastrutture strategiche.

Forescout Device Cloud

La soluzione NAC di Forescout mette a disposizione dei propri clienti un motore (Forescout Device Cloud) che alimenta la classificazione automatica della piattaforma e assicura che questa ricca fonte di informazioni rimanga all'altezza di gestire l'aumento e la diversificazione dei dispositivi.

Grazie all'analisi di oltre 12 milioni di dispositivi dei propri clienti Forescout Device Cloud è il più grande data-lake al mondo di informazioni provenienti dai dispositivi, un'unica fonte attendibile e intersettoriale di impronte digitali, comportamenti e profili di rischio di tutte le singole risorse presenti nella tua rete.

Forescout Research Lab pubblica frequentemente nuovi profili al fine di migliorare efficacia, copertura e velocità nella classificazione nell'intero panorama dei dispositivi.

Valutazione dello stato in modalità Agentless e remediation automatica

La fase di classificazione comunica il contesto operativo e la finalità di un dispositivo: in pratica indica di che tipo di dispositivo si tratta. Per ottenere una visione completa, tuttavia, è necessario disporre di un altro strumento che determini l'integrità di ciascun dispositivo.

La piattaforma NAC di Forescout monitora continuamente la rete e valuta la configurazione, la condizione e lo stato di sicurezza dei dispositivi connessi per determinarne i profili di rischio, la conformità alle normative e la loro adesione alle policy di sicurezza.

Forescout risponde a domande importanti, quali, ad esempio:

- I dispositivi utilizzano sistemi operativi approvati e aggiornati con le ultime patch?
- Il software di sicurezza è installato, operativo e aggiornato con le ultime patch?
- Ci sono dei dispositivi che eseguono applicazioni non autorizzate o che violano gli standard di configurazione?
- I dispositivi utilizzano password predefinite o elementari (situazione particolarmente rischiosa per i dispositivi IoT)?

- Sono stati rilevati dispositivi inaffidabili, compresi quelli che si spacciano per legittimi tramite tecniche di spoofing?
- Quali dei dispositivi connessi sono più vulnerabili alle ultime minacce?

Dopo aver risposto a queste domande fondamentali, la piattaforma NAC di Forescout impone la conformità ai dispositivi automatizzandone il processo di remediation per mezzo di comandi nativi o di terze parti.

Importanti nuove funzionalità sono state recentemente introdotte all'interno della piattaforma:

- Garantire la corretta configurazione degli endpoint e avviare il processo di remediation per le violazioni critiche alla configurazione, incluse password predefinite o non sicure;
- Assicurare costantemente che gli agent di sicurezza stiano funzionando correttamente (che siano installati, correttamente in esecuzione e aggiornati);
- Disabilitare o bloccare applicazioni non autorizzate che potrebbero introdurre rischi o gravare inutilmente sulla larghezza di banda della rete o sulla produttività delle risorse;
- Identificare vulnerabilità ad alto rischio e patch critiche mancanti e avviare le corrispondenti azioni correttive;
- Avviare azioni di correzione preventive come l'installazione dei software di sicurezza necessari, l'aggiornamento degli agent o l'applicazione delle patch di sicurezza;
- Implementare policy e automatizzare i controlli per la conformità della configurazione nelle distribuzioni cloud, tra cui AWS, Azure e VMware.

La visibilità è la chiave per il controllo

Ogni cliente ha una rete differente, è per questo che le rispettive esigenze variano e le policy di sicurezza sono univoche, ed è quindi fondamentale distribuire una soluzione flessibile, che metta in sicurezza tutte le reti: cablate, wireless e VPN.

Per esempio, nelle proprie reti cablate le grandi imprese impiegano solitamente la soluzione NAC di Forescout senza l'uso del protocollo IEEE802.1X. Scelgono questa opzione perché è facile da distribuire, non richiede di effettuare l'upgrade dell'infrastruttura hardware/software, né complesse configurazioni di switch o endpoint, come il protocollo IEEE 802.1X normalmente richiede, e funziona nelle infrastrutture di rete dove sono presenti uno o più vendor diversi.

Questa prassi è coerente con le raccomandazioni di Gartner di non utilizzare la modalità di autenticazione basata sul protocollo IEEE 802.1X nelle reti cablate, se si desidera una distribuzione più semplice e minori costi operativi.

Nelle reti wireless, la prassi normale è quella di impiegare l'autenticazione basata sul protocollo IEEE 802.1X per i dispositivi informatici degli utenti aziendali.

Le opzioni di distribuzione ibride e flessibili della soluzione NAC di Forescout supportano facilmente entrambe queste modalità operative contemporaneamente sulle stesse infrastrutture aziendali.

Di seguito sono elencati alcuni dei principali vantaggi derivanti dall'utilizzo della piattaforma NAC di Forescout per la protezione dell'accesso alla rete:

a) **Maggiore flessibilità:**

   i) Ampia gamma di metodi per il controllo degli accessi, con o senza l'utilizzo del protocollo IEEE 802.1X.

   ii) Architettura cablata robusta pur senza l'uso di IEEE802.1X: non intrusiva, facile da impiegare, con minima configurazione, nessun upgrade dell'infrastruttura, opzioni per il supporto della funzione di controllo accessi in modalità pre-connect o post-connect, immediata redditività e rapido ritorno sull'investimento.

   iii) Motore delle policy unificato per implementare un accesso differenziato (ospite, BYOD, aziendale, IoT) e sicuro con Zero Trust.

b) Nessun upgrade:

   i) Funziona con l'infrastruttura esistente senza dover effettuare l'upgrade di software/hardware.

   ii) È in grado di operare con il vendor scelto per l'infrastruttura della rete (per esempio, switch, controller wireless, IaaS), riducendo la dipendenza dal produttore e massimizzando la redditività e permettendo un ritorno dell'investimento più rapido.

c) Eterogeneità:

   i) L'integrazione diretta (tramite SNMP, SSH, Telnet, RADIUS) con centinaia di switch e controller wireless di oltre 40 fornitori di infrastruttura di rete, con sistemi operativi di differenti versioni consente di controllare gli accessi in qualsiasi rete di tipo multivendor.

   ii) La soluzione, flessibile e non intrusiva, è in grado di abbassare i costi di distribuzione, manutenzione e operativi.

iii) Il supporto di reti eterogenee permette inoltre di ottenere rapidamente funzioni di visibilità e controllo sulle risorse nel caso di una fusione o dell'acquisizione di eventuali nuove subsidiaries.

d) Segmentazione:

La soluzione NAC di Forescout è dotabile anche di un modulo che sfrutta le informazioni di visibilità offerta dalla piattaforma per comprendere lo stato della segmentazione della rete in tempo reale e su qualsiasi dispositivo.

Tramite il modulo di segmentazione si è quindi in grado di progettare e simulare le policy di segmentazione logica all'interno della rete in modo da valutarne l'impatto prima di applicarle.

Tramite il modulo di segmentazione si è in grado di monitorare in tempo reale l'integrità della segmentazione della rete e reagire alle eventuali violazioni delle policy in tutta la rete aziendale.

e) Coordinamento con i prodotti informatici e di sicurezza:

Durante l'intero processo di controllo degli accessi alla rete, la soluzione NAC di Forescout può funzionare insieme ai pe-esistenti strumenti di sicurezza scambiando in modalità bidirezionale, in tempo reale, il contesto dei dispositivi e le relative notifiche di elaborazione dei dati, automatizzando i flussi di lavoro delle risposte agli incidenti di sicurezza informatica. Ciò non solo accelera la mitigazione del rischio, ma ti consente anche di massimizzare il ritorno dell'investimento nei prodotti di sicurezza informatica preesistenti.

Grazie alle integrazioni pronte all'uso di eyeExtend e all'app eyeExtend Connect, aiutiamo i clienti a trasformare rapidamente la gestione della sicurezza, passando da silos isolati a un sistema di risposta integrato ed automatizzato che, su scala aziendale, difende attivamente la tua Enterprise of Things.

Di seguito sono elencati alcuni dei benefici derivanti dal coordinamento con gli strumenti di sicurezza preesistenti durante la procedura di controllo degli accessi (NAC):

- **Condivisione del contesto dei dispositivi**

Il contesto dei dispositivi viene condiviso con gli strumenti di gestione delle risorse per assicurare di avere sempre l'inventario più aggiornato e più accurato (CMDB). Inoltre, in tempo reale, il contesto dei dispositivi viene fornito agli addetti alla sicurezza e alle applicazioni per la correlazione e l'assegnazione delle priorità agli eventi.

- **Avviamento dei flussi di lavoro alla connessione**

Gli strumenti esistenti potrebbero non valutare la vulnerabilità dei dispositivi transitori a causa di scansioni sporadiche (come nel caso dei sistemi di Vulnerability Assesment). La soluzione NAC di Forescout opera con gli strumenti di sicurezza per attivare le scansioni delle vulnerabilità in tempo reale al momento delle connessioni su specifici endpoint individuati ed avvia l'applicazione delle patch e gli aggiornamenti della protezione nel momento della connessione alla rete dell'endpoint al fine di ridurre la superficie di attacco.

- **Valutazione dello stato di sicurezza**

Verifica che gli agent di sicurezza esistenti siano funzionanti, identifica i dispositivi che presentano rischi e IoC (Indicatori di Compromissione) e rileva gli account con privilegi, ma illegittimi od obsoleti, nei dispositivi che si connettono.

- **Azioni di risposta automatizzate**

Argina, mette in quarantena o blocca i dispositivi vulnerabili, compromessi e ad alto rischio ed avvia le azioni di mitigazione e correzione basate sulle policy per la risposta agli incidenti

Configurazioni in Convenzione

Nella convenzione Consip LAN 7 sono presenti configurazioni della tecnologia NAC di Forescout Technologies in grado di coprire, come richiesto dalla convenzione stessa, le seguenti tipologie di dimensionamento:

1) NAC Fascia Base - Fino a 100 Endpoint concorrenti – In fase di sostituzione per End of Sale
2) NAC Fascia Media - Fino a 500 Endpoint concorrenti
3) NAC Fascia Alta - Fino a 1000 Endpoint concorrenti
4) NAC Fascia Top - Fino a 10000 Endpoint concorrenti
5) NAC Fascia Top Macchina Virtuale - Fino a 10000 Endpoint concorrenti senza appliance HW

Ciascuna delle configurazioni suddette comprende le licenze atte a garantire le funzionalità seguenti:

1) Visibilità degli endpoint;
2) Asset Management relativo agli endpoint individuati;
3) Device Compliancy degli endpoint individuati con le policy definite dall'utente;
4) Policy Enforcement delle azioni correttive definite dall'utente;
5) Integrazione con un brand di firewalling tra quelli indicati nella documentazione tecnica di gara;

6) Integrazione con un brand di Mobile Device Management tra quelli indicati nella documentazione tecnica di gara;

7) Appliance HW ad esclusione della configurazione prevista in sola modalità virtuale.

4.8. Security E-mail Gateway

4.8.1. Fortinet

La soluzione Fortinet per la protezione del traffico e-mail è basata sul prodotto FortiMail. Le funzionalità di sicurezza di FortiMail utilizzano le tecnologie e i servizi di sicurezza più recenti di FortiGuard Labs per offrire una protezione di livello costantemente elevato dalle minacce comuni e avanzate, integrando al contempo solide funzionalità di protezione dei dati per evitarne la perdita.

Le organizzazioni in genere scelgono la sicurezza e-mail offerta da FortiMail per proteggere gli utenti e, in ultima analisi i dati, da un'ampia gamma di minacce informatiche quali: volumi sempre crescenti di spam indesiderato, phishing basato su tecniche di ingegneria sociale, compromissione di e-mail aziendali, accelerazione delle varianti di ransomware e altri malware, attacchi sempre più mirati da parte di malintenzionati di ogni tipo e altro ancora. Al tempo, FortiMail può essere utilizzato per proteggere dati di tutti i tipi, riducendo il rischio di perdite involontarie e/o mancata conformità a normative come HIPAA, PCI, GDPR e altre.

Le principali caratteristiche di FortiMail sono:

- Antispam e antiphishing di alto livello; protegge gli utenti finali da spam indesiderato e dannosi attacchi di phishing
- Difesa avanzata dalle minacce certificata da enti indipendenti; contrasta i cybercriminali intenzionati a sottrarre dati, tenere sistemi in ostaggio con il ransomware, portare a termine frodi e perseguire altri scopi dolosi
- Protezione dei dati integrata; protegge la privacy delle informazioni personali e la riservatezza dei dati sensibili in conformità alle linee guida normative e aziendali
- Gestione di classe enterprise; consente al personale e agli utenti finali di dedicarsi al business riducendo il tempo necessario per la gestione delle e-mail
- Alte prestazioni di gestione e-mail; velocizza il recapito delle e-mail legittime con un ottimo TCO (Total Cost of Ownership).

Dispositivo SEG fascia base

Il dispositivo proposto per i SEG Fascia Base è il FortiMail-200F.

Di seguito sono riportati i requisiti minimi e migliorativi richiesti nella gara per i dispositivi SEG di fascia base:

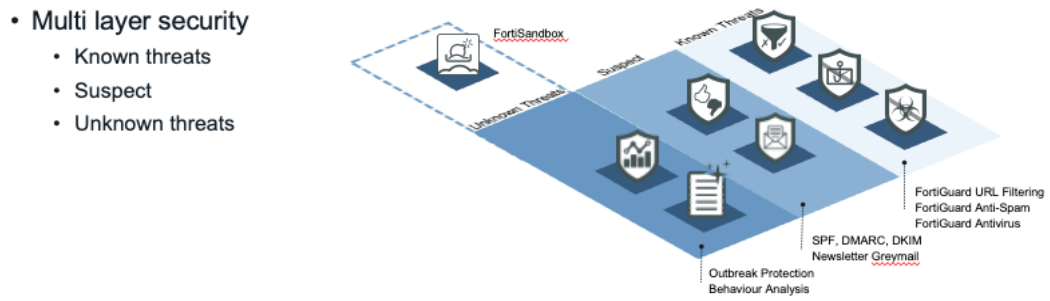
- Message transfer agent (MTA)

- Gestione quarantena
- Funzionalità anti-malware signature based
- Funzionalità antispam
- Gestione e-mail massive
- Gestione fino a 45.000 e-mail per ora; i valori di throughput in termini di e-mail per ora sono da considerarsi calcolati nelle condizioni in cui l'apparato abbia attiva la funzionalità antivirus e antispam.

I requisiti migliorativi sono i seguenti:

- Funzionalità di Data loss prevention
- Funzionalità di E-mail Encryption
- Funzionalità di Antispoofing, Antiphishing Protezione da messaggi di posta elettronica contenenti URL malevoli
- Integrazione con almeno un servizio di sandbox in cloud e/o almeno un prodotto di sandbox offerto

Il prodotto FortiMail FML-200F supporta sia i requisiti di base che i requisiti migliorativi attraverso l'integrazione con la FortiSandbox 1000F in offerta. L'utilizzo di FortiMail e FortiSandbox è una integrazione particolarmente consigliata dal punto di vista della cybersecurity perché permette di proteggere il paziente zero, cioè non far arrivare all'utente mail virate e sospette.



FortiMail 200F viene offerto con FortiGuard Base Bundle (Forticare, FortiGuard AS & AV, FortiGuard Virus Outbreak Protection, Identity Based Encryption, Data Loss Prevention).

Sono inoltre disponibili ulteriori funzionalità di sicurezza non previste in convenzione, che prevedono licenze a parte.

La tabella seguente riassume le performance del FortiMail FML-200F

Performance di Sistema

Protected Email Domains	20
Server Mode Mailboxes	150
E-mail Routing (Msg/hr) (Basato su messaggi da 100KB, no queueing)	50.000
E-mail Routing (Msg/hr) AV + AS	45.000
FortiGuard Enterprise ATP (Msg/hr) (Basato su messaggi da 100KB, no queueing)	30.000
Porte GE RJ45	4
Capacità di storage	1x1TB
Form Factor	1RU

Riferimenti documentali pubblici:

https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiMail.pdf

Dispositivo SEG fascia media

Il dispositivo proposto per i SEG Fascia Media è il FortiMail-400F.

Di seguito sono riportati i requisiti minimi e migliorativi richiesti nella gara per i dispositivi SEG di fascia base:

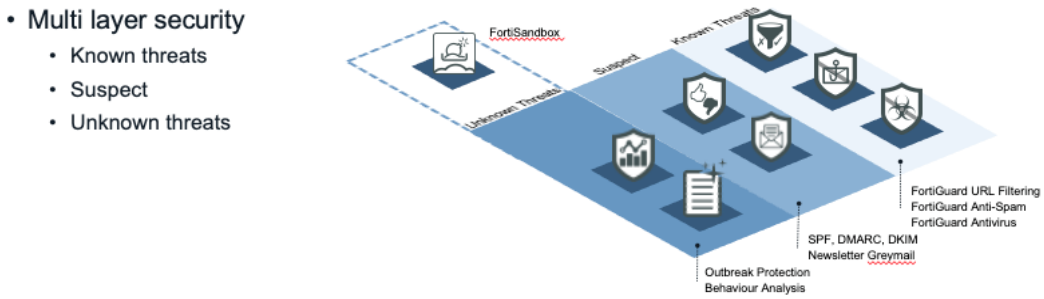
- Message transfer agent (MTA)
- Gestione quarantena
- Funzionalità anti-malware signature based
- Funzionalità antispam
- Gestione e-mail massive
- Gestione fino a 90.000 e-mail per ora; i valori di throughput in termini di e-mail per ora sono da considerarsi calcolati nelle condizioni in cui l'apparato abbia attiva la funzionalità antivirus e antispam.

I requisiti migliorativi sono i seguenti:

- Funzionalità di Data loss prevention

- Funzionalità di E-mail Encryption
- Funzionalità di Antispoofing, Antiphishing Protezione da messaggi di posta elettronica contenenti URL malevoli
- Integrazione con almeno un servizio di sandbox in cloud e/o almeno un prodotto di sandbox offerto

Il prodotto FortiMail FML-400F supporta sia i requisiti di base che i requisiti migliorativi, attraverso l'integrazione con la FortiSandbox 1000F in offerta. L'utilizzo di FortiMail e FortiSandbox è una integrazione particolarmente consigliata dal punto di vista della cybersecurity perché permette di proteggere il paziente zero, cioè non far arrivare all'utente mail virate e sospette.



FortiMail 400F viene offerto con FortiGuard Base Bundle (Forticare, FortiGuard AS & AV, FortiGuard Virus Outbreak Protection, Identity Based Encryption, Data Loss Prevention).

Sono inoltre disponibili ulteriori funzionalità di sicurezza non previste in convenzione, che prevedono licenze a parte.

La tabella seguente riassume le performance del FortiMail FML-400F

Performance di Sistema	
EProtected mail Domains	100
Server Mode Mailboxes	400
E-mail Routing (Msg/hr) (Basato su messaggi da 100KB, no queueing)	250.000
FortiGuard Enterprise ATP (Msg/hr) (Basato su messaggi da 100KB, no queueing)	90.000
Porte GE RJ45	4

Capacità di storage	2x1TB
Form Factor	1RU

Riferimenti documentali pubblici:

https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiMail.pdf

4.8.2. Sonicwall

La posta elettronica è fondamentale per la comunicazione aziendale, ma è anche il principale vettore delle minacce come ransomware, phishing, business e-mail compromise (BEC), spoofing, spam e virus. Inoltre, in base alle normative vigenti, è responsabilità dell'azienda proteggere i dati riservati impedendo eventuali perdite di dati e assicurare lo scambio sicuro di e-mail contenenti informazioni riservate o dati sensibili dei clienti. Le organizzazioni di ogni dimensione, dalle PMI in crescita alle grandi aziende con ambienti distribuiti fino ai fornitori di servizi gestiti (MSP), necessitano di una soluzione a costi contenuti che garantisca la sicurezza e la crittografia dei messaggi di posta elettronica e la modularità necessaria per aumentare agevolmente la capacità delle unità organizzative e dei domini delegando la gestione.

Il software e le apparecchiature SonicWall Email Security offrono una protezione multilivello dalle minacce e dalle violazioni di conformità provenienti dall'interno e dall'esterno attraverso la posta elettronica, effettuando la scansione dei dati sensibili in tutti i contenuti, gli URL e gli allegati dei messaggi di posta elettronica in entrata e in uscita, offrendo una protezione in tempo reale contro ransomware, attacchi di phishing mirati, spoofing, virus, URL dannosi, zombi, attacchi Directory Harvest (DHA), Denial of Service (DoS) e altri. La soluzione sfrutta tecniche multiple di rilevamento delle minacce brevettate di SonicWall e un'esclusiva rete internazionale di identificazione e monitoraggio degli attacchi.

Il servizio SonicWall Capture Advanced Threat Protection prevede il sandboxing multi-engine leader del settore, con tecnologia RTDMI™ (Real-Time Deep Memory Inspection) in attesa di brevetto, per isolare le minacce sconosciute riscontrate in URL e file allegati sospetti, consentendo di bloccare le minacce avanzate prima che arrivino nelle caselle di posta degli utenti. La soluzione E-mail Security abbinata a Capture ATP offre una difesa decisamente efficace e tempestiva nei confronti del ransomware e degli attacchi zero-day.

La soluzione comprende anche DKIM (Domain Keys Identified Mail), SPF (Sender Policy Framework) e Domain-based Message Authentication, Reporting and Conformance (DMARC), un potente metodo di autenticazione dei messaggi di posta elettronica che contribuisce a individuare i messaggi di posta falsificati, riducendo lo spam e gli attacchi di phishing mirati come spear-phishing, whaling, truffa del CEO e compromissione delle e-mail aziendali. Inoltre, questo metodo segnala la provenienza e i mittenti dei messaggi di posta elettronica, consentendo di individuare e bloccare mittenti non autorizzati che falsificano i messaggi con l'indirizzo dell'azienda e di proteggere il vostro marchio. Inoltre, impedisce la perdita di dati riservati e le violazioni

normative con una scansione e una gestione che garantiscano la conformità avanzata, compreso il servizio integrato di crittografia dei messaggi nel cloud per garantire lo scambio sicuro di dati sensibili.

La soluzione E-mail Security è intuitiva, rapida e semplice da gestire. La gestione dello spam può essere delegata agli utenti finali, mantenendo comunque il massimo controllo sull'applicazione della sicurezza. Inoltre, la sincronizzazione con più server LDAP senza soluzione di continuità consente di gestire facilmente gli account degli utenti e dei gruppi. In ambienti distribuiti di grande estensione, il supporto multi-tenancy consente di delegare ad amministratori subordinati la gestione delle impostazioni su più unità organizzative (come divisioni aziendali o clienti MSP) all'interno di un'unica installazione di E-mail Security.

Vantaggi

- Impediscono al ransomware e al malware zero-day di raggiungere la casella di posta grazie a Capture Advanced Threat Protection;
- Impediscono agli utenti di fare clic su link nocivi da qualsiasi dispositivo e da qualsiasi sede grazie alla protezione time-of-click degli URL;
- Utilizzano tecniche di analisi avanzate per bloccare gli attacchi di phishing mirati, le frodi via e-mail e la compromissione delle e-mail aziendali (BEC);
- Bloccano le nuove minacce grazie agli aggiornamenti dell'intelligenza delle minacce in tempo reale forniti da SonicWall Capture Labs;
- Mantengono l'igiene della posta elettronica grazie a potenti anti-spam e antivirus;
- Proteggono i dati attuando la prevenzione granulare della perdita dei dati (DLP) e politiche di conformità;
- Semplificano la gestione grazie all'automazione intelligente, alla delega dei processi, al pannello di controllo facilmente personalizzabile e ad una reportistica avanzata;
- Utilizzano opzioni di installazione flessibili e modulari, tra cui apparecchiature fisiche hardened, apparecchiature virtuali robuste e un potente software Windows Server.

Protezione contro le minacce avanzate

Individuare e bloccare le minacce avanzate fino al verdetto. Questo è l'unico servizio di individuazione delle minacce avanzate che combina il sandboxing multilivello, inclusi la tecnologia Real-Time Deep Memory Inspection, l'emulazione completa del sistema e tecniche di virtualizzazione, per analizzare il comportamento del codice sospetto nei messaggi di posta elettronica e proteggere i clienti dai crescenti pericoli delle minacce zeroday.

Il servizio prevede la protezione avanzata degli URL, che analizza dinamicamente gli URL integrati in modo da bloccare e mettere in quarantena messaggi con URL dannosi prima che raggiungano le caselle di posta evitando che gli utenti possano fare clic su di essi, con conseguente compromissione.

Il servizio Capture ATP offre una migliore granularità, con l'analisi dei file allegati e degli URL, ulteriori capacità per la creazione di report dettagliati e un'esperienza utente razionalizzata.

SonicWall E-mail Security riscrive altresì tutti gli URL incorporati per bloccare i messaggi di posta elettronica contenenti URL di phishing o dannosi; in questo modo, gli utenti sono protetti al momento del clic su qualsiasi dispositivo e da qualunque sede. Alcune organizzazioni ed enti pubblici non possono utilizzare tecniche basate su cloud per il controllo dei file, come Capture ATP, per ragioni di conformità o di latenza. Integrate le vostre apparecchiature E-mail Security con le apparecchiature SonicWall Capture Security (CSa) per esaminare direttamente nel vostro datacenter i file sospetti che arrivano attraverso la posta elettronica. CSa può essere referenziato mediante indirizzo IP o FQDN, il che ne fa un'ottima risorsa per la prevenzione delle minacce.

Protezione dagli attacchi mirati

La tecnologia anti-phishing di SonicWall usa una combinazione di metodologie quali apprendimento automatico, euristica e analisi della reputazione e del contenuto per bloccare attacchi di phishing sofisticati. La soluzione prevede anche potenti standard di autenticazione della posta elettronica come SPF, DKIM e DMARC per bloccare attacchi di spoofing, compromissione delle e-mail aziendali e frodi via e-mail.

Intelligenza delle minacce in tempo reale

Beneficiate della protezione più approfondita e aggiornata contro i nuovi attacchi di spam, che garantisce al tempo stesso la consegna dei messaggi di posta elettronica legittimi con informazioni sulle minacce in tempo reale provenienti da SonicWall Capture Threat Network, che raccoglie i dati da milioni di fonti. SonicWall Capture Labs analizza queste informazioni ed esegue rigorosi test, assegnando poi un punteggio alla reputazione di mittenti e contenuti per individuare le nuove minacce in tempo reale.

Protezione antivirus e antispyware

Beneficiate di una protezione aggiornata antivirus e antispyware. La soluzione utilizza segnature provenienti dai principali database antivirus del settore e il rilevamento degli URL dannosi per offrire una protezione multilivello superiore a quella offerta dalle soluzioni che si basano su singole tecnologie antivirus.

Inoltre, l'analisi predittiva consente di proteggere la rete quando si diffonde un nuovo virus fino a quando non viene reso disponibile l'aggiornamento della segnatura antivirus.

Automazione intelligente, delega dei processi e reportistica avanzata

Semplificate la gestione grazie all'automazione intelligente, alla delega dei processi e ad una reportistica avanzata. Gestite automaticamente i gruppi di utenti, gli account e gli indirizzi di posta elettronica. Beneficiate

di un'integrazione avanzata con più server LDAP. Delegate con fiducia la gestione dello spam agli utenti finali grazie al plug-in scaricabile del pulsante di posta indesiderata di Outlook®, mantenendo allo stesso tempo il pieno controllo locale. Individuate qualsiasi messaggio di posta nel giro di pochi secondi con il Rapid Message Search Engine. La reportistica centralizzata (anche in modalità split) fornisce informazioni granulari a livello dell'intero sistema, facilmente personalizzabili sui tipi di attacchi, sull'efficacia delle soluzioni e sul monitoraggio integrato delle prestazioni, con reportistica disponibile in formato PDF e JPEG.

Gestione delle politiche di conformità

Questo servizio aggiuntivo consente la conformità con gli obblighi normativi aiutandovi a individuare, monitorare e segnalare i messaggi di posta elettronica che violano le normative e le linee guida in materia di conformità (es., HIPAA, SOX, GLBA e PCI-DSS) e le linee guida aziendali sulla perdita di dati. Inoltre, il servizio in abbonamento consente l'instradamento basato sulle politiche della posta per approvazione, archiviazione e crittografia.

Crittografia dei messaggi di posta elettronica

Utilizzate una potente struttura per impedire la perdita di dati, gestire e attuare i requisiti di conformità e consentire uno scambio sicuro dei messaggi compatibili con i dispositivi mobili.

I messaggi crittografati possono essere monitorati per sapere quando vengono recapitati e aperti. Il destinatario riceverà un intuitivo messaggio di notifica con semplici istruzioni per accedere a un portale sicuro in cui leggere o scaricare il messaggio in tutta tranquillità. Il servizio è basato su cloud e non necessita di software client aggiuntivo, e diversamente dalle soluzioni della concorrenza i messaggi crittografati sono accessibili e possono essere letti dai dispositivi mobili e dai portatili.

Opzioni di installazione flessibili

Ottenete valore modulare a lungo termine configurando la vostra soluzione in funzione della crescita e della ridondanza con minimi costi iniziali. È possibile installare E-mail Security come apparecchiatura hardened dalle prestazioni elevate, come software che sfrutta l'infrastruttura esistente o come apparecchiatura virtuale che sfrutta le risorse di calcolo condivise per ottimizzare l'utilizzo, facilitare la migrazione e ridurre i costi di investimento. Iniziate con un sistema singolo e man mano che la vostra azienda cresce aggiungete capacità e passate a un'architettura in modalità split e abilitata per il fail-over. La compatibilità multi-tenancy consente alle grandi aziende o ai fornitori di servizi gestiti di effettuare installazioni in più dipartimenti o clienti per istituire unità organizzative con uno o più domini. L'installazione può essere gestita centralmente, pur consentendo alle singole unità organizzative di avere in proprio utenti, sub-amministratori, regole di politica, caselle di posta indesiderata e altro ancora.

Opzioni di installazione di SonicWall E-mail Security

L'architettura decisamente flessibile di SonicWall E-mail Security consente l'installazione in organizzazioni che richiedono una soluzione altamente modulare, ridondante e distribuita per la protezione della posta elettronica gestibile centralmente. SonicWall E-mail Security può essere installata in modalità all-in-one o in modalità split.

In modalità split, i sistemi possono essere configurati come analizzatore remoto o centro di controllo. In una tipica configurazione in modalità split, uno o più analizzatori remoti sono collegati a un centro di controllo. L'analizzatore remoto riceve i messaggi di posta elettronica da uno o più domini e applica tecniche di gestione delle connessioni, filtraggio dei messaggi (antispam, anti-phishing e antivirus) e politiche avanzate per consegnare i messaggi legittimi ai server di posta elettronica a valle. Il centro di controllo gestisce centralmente tutti gli analizzatori remoti e acquisisce e memorizza i messaggi indesiderati provenienti dagli stessi. La gestione centralizzata comprende funzioni di reportistica e monitoraggio di tutti i sistemi correlati. Questo paradigma consente la modularità della soluzione con un valido rapporto costi-benefici e protegge i messaggi di posta elettronica in entrata e in uscita per le organizzazioni in crescita. Utilizzando le apparecchiature virtuali SonicWall E-mail Security, la modalità split può essere completamente installata su uno o più server per un'ottimale efficienza di scala.

Funzioni presenti

Protezione time-of-click degli URL	Sì
Abbonamento Total Secure – Pacchetto di protezione di base	
Comprende un abbonamento 24x7 alla protezione dinamica della posta elettronica più antivirus multilivello, rilevamento degli URL dannosi e gestione della conformità in abbonamento	Sì
Protezione completa dei messaggi di posta elettronica in entrata e in uscita	
Anti-spam	Sì
Gestione delle connessioni con reputazione IP avanzata	Sì
Rilevamento, classificazione e blocco del phishing	Sì
Protezione contro Directory Harvest, Denial of Service e NDR	Sì
Anti-spoofing con supporto per SPF, DKIM e DMARC	Sì

Regole di politica per utenti, gruppi, tutti	Sì
MTA (Message Transfer Agent) in memoria per una maggiore velocità	Sì
Facilità di amministrazione	
Installazione	< 1 ora
Interventi di gestione settimanali	< 10 min
Sincronizzazione automatica multi-LDAP per utenti, gruppi	Sì
Compatibilità con tutti i server di posta elettronica SMTP	Sì
Compatibilità autenticazione SMTP (SMPT AUTH)	Sì
Autorizzazione/rifiuto dei controlli per utenti finali	Sì
Personalizzazione, programmazione e invio per posta elettronica di oltre 30 rapporti	Sì
Particolari sulle valutazioni	Sì
Pannello di controllo facilmente personalizzabile	Sì
Rapid Message Search Engine	Sì
Architettura modulare in modalità split	Sì
Clustering e clustering remoto	Sì
Facilità per gli utenti finali	
Single Sign-On	Sì

Caselle di posta indesiderata per i singoli utenti e riepilogo posta indesiderata	Sì
Definizione delle impostazioni di spam per singoli utenti, elenchi blocchi/autorizzazioni	Sì
Abbonamento alla protezione dei messaggi di posta elettronica con supporto dinamico necessario	
Aggiornamenti automatici antivirus, antispam, anti-phishing SonicWall nel cloud ogni minuto	Sì
Supporto 24x7	Sì
RMA (sostituzione dell'apparecchiatura)	Sì
Aggiornamenti software/firmware	Sì
Abbonamento anti-virus	
Feed segnature dai principali database antivirus del settore	Sì
Anti-virus SonicWall TimeZero	Sì
Rilevamento zombi	Sì
Abbonamento Email Encryption	
Possibilità di abbonamento Compliance più crittografia dei messaggi di posta elettronica basata sulle politiche e scambio sicuro dei messaggi	Sì

Specifiche del sistema

APPARECCHIATURE SECURITY	EMAIL 5000		7000

Chassis per montaggio a rack	1RU	1RU
CPU	Celeron G1820	i3-4330
RAM	8 GB	16 GB
Disco rigido	500 GB	1 TB
Redundant disk array (RAID)	—	RAID 1
Unità sostituibili a caldo	No	Sì
Alimentazione ridondante	No	No
SAFE Mode Flash	Sì	Sì
Dimensioni	17,0 x 16,4 x 1,7 pollici (43,18 x 41,59 x 4,44 cm)	17,0 x 16,4 x 1,7 pollici (43,18 x 41,59 x 4,44 cm)
Peso	16 libbre / 7,26 kg	16 libbre / 7,26 kg
Peso RAEE	16 libbre / 7,37 kg	16 libbre / 22,2 kg
Potenza assorbita (Watt)	46	48
BTU	155	162
MTBF @25C in ore	130.919	150.278
MTBF @25C in anni	14,9	17,2

5. Gruppi di continuità

Un gruppo di continuità, chiamato anche con UPS Uninterruptible Power Supply, è un'apparecchiatura elettrica utilizzata per ovviare a repentine anomalie nella erogazione di energia elettrica normalmente utilizzata per alimentare apparati tecnologici e ridurre il rischio di interruzioni di servizio derivanti dalla temporanea assenza della rete primaria. I gruppi di continuità sono utilizzati per erogare costantemente una forma d'onda perfettamente sinusoidale alla frequenza di oscillazione prefissata, priva di variazioni accidentali che potrebbero perturbare il corretto funzionamento delle apparecchiature alimentate.

La sua caratteristica peculiare è che - all'accadere di una grave avaria nella fornitura elettrica in ingresso - limita l'assenza di corrente alle apparecchiature collegate alla sua uscita in tempo sostanzialmente pari a zero o a pochissimi millisecondi.

Gli UPS in genere sono in grado di fornire energia elettrica per un lasso di tempo piuttosto breve ("tempo di back-up"), ma l'autonomia generata dalle batterie entro-contenute può essere incrementata mediante espansioni opzionali.

La configurazione degli UPS può essere di tipo desk tower, con esecuzione a pavimento, oppure tower/rack convertibile. Nel secondo caso i gruppi di continuità possono essere facilmente installati in armadi tecnici a passo standard 19", mediante l'ausilio di alette di fissaggio frontali fornite a corredo del gruppo di continuità.

La norma IEC EN 62040-3 definisce la topologia dei gruppi di continuità in base alla loro dipendenza dalla corrente in ingresso, alla qualità della forma d'onda che viene erogata.

La suddivisione in VFI, VI ricalca indirettamente le due tipologie costruttive principali, e cioè On-Line, Line-Interactive la sigla è riferita alle condizioni di normale esercizio (presenza di idonea fornitura elettrica all'ingresso dell'UPS, quindi nessun utilizzo delle batterie), ed indica le caratteristiche della corrente in uscita dall'UPS in relazione a quella in ingresso:

- VFI "Voltage and Frequency Independent" (tensione e frequenza indipendente): tensione, frequenza (e forma d'onda) in uscita sono rigenerati dall'UPS tramite il passaggio della corrente in ingresso attraverso raddrizzatore e inverter. Questi UPS sono anche detti On-Line doppia conversione. Rappresentano tipicamente la migliore garanzia contro i rischi derivanti di interruzione di servizio.
- VI "Voltage Independent" (tensione indipendente): la tensione in uscita è corretto rispetto a quello in ingresso (tramite AVR), mentre la frequenza (e la forma d'onda) è la stessa. Questi UPS sono anche detti Line Interactive.

Per favore la massimizzazione del risparmio energetico, in ottica di riduzione dei consumi di energia, gli UPS di ultima generazione sono dotati di una modalità di funzionamento denominata ECO-Mode, che favorisce un sostanziale contenimento dei consumi durante il normale funzionamento del gruppo di continuità.

Tutti gli UPS proposti in sede di offerta, sono pienamente rispondenti al capitolato di gara o, in taluni casi, migliorativi dal punto di vista dei requisiti prestazionali.

Tutti gli UPS in convenzione devono prevedere un hardware dedicato (Scheda di rete con interfaccia Ethernet RJ45), tale da garantire la supervisione remota secondo lo standard SNMP. In informatica e telecomunicazioni Simple Network Management Protocol (SNMP) è un protocollo di rete senza connessione che appartiene alla suite di protocolli Internet definito dalla IETF. Nello specifico, è previsto il requisito nella sezione Capitolato Tecnico § 2.4 Gruppi di Continuità di seguito richiamata:

RIFERIMENTO AL CAPITOLATO TECNICO	REQUISITI MINIMI	CONFORME
Capitolato Tecnico § 2.4 Gruppi di Continuità	fattore di potenza ≥ 0.9 (in uscita) per i tagli da 1000VA a 3000VA; fattore di potenza = 1 (in uscita) per i tagli da 5000VA a 40000VA.	Sì
	Software per spegnimento automatico delle apparecchiature	Sì
	Possibilità di aumento della potenza in caso di "upgrade" degli armadi con nuovi apparati	Sì
	Scheda di rete con interfaccia Ethernet RJ45 e funzionalità di monitoraggio tramite protocollo SNMP (v2 o migliorativa)	Sì
	Rispondenza alla normativa EN 62040-x	Sì
	Tipologia VI-SS-122 secondo EN 62040-3 per i tagli da 1000VA a 3000VA. Tipologia VFI-SS-111 secondo EN62040-3 per gli tagli da 5000VA a 40000VA	Sì
	per i gruppi di continuità da 5.000VA in su, scheda di parallelo integrata per parallelabilità minima di 3 unità ordinabile opzionalmente dalla singola Unità Ordinante	Sì
	Funzionalità eco mode	Sì

Modelli proposti

GRUPPI DI CONTINUITÀ		
Identificazione del prodotto offerto	**Marca**	**Modello**
Tipo convertibile tower/rack con capacità di circa 1000VA	POWERME	VI MM9 1K
Tipo convertibile tower/rack con capacità di circa 1500VA	POWERME	VI MM9 1,5K
Tipo convertibile tower/rack con capacità di circa 2000VA	POWERME	VI MM9 2K
Tipo convertibile tower/rack con capacità di circa 3000VA	POWERME	VI MM9 3K
Tipo convertibile tower/rack con capacità di circa 5000VA	POWERME	GPMM 6K(L) RT-LV
Tipo convertibile tower/rack con capacità di circa 10000VA	POWERME	GPMM 10K(L) RT-LV
Tipo tower con capacità di circa 15000VA	POWERME	TPTM 1 3/1 15K

Tipo tower con capacità di circa 20000VA	POWERME	TPTM 1 3/1 20K
Tipo tower con capacità di circa 10000VA trifase/trifase	POWERME	TPTT 1 10K
Tipo tower con capacità di circa 15000VA trifase/trifase	POWERME	TPTT 1 15K
Tipo tower con capacità di circa 20000VA trifase/trifase	POWERME	TPTT 1 20K
Tipo tower con capacità di circa 40000VA trifase/trifase	POWERME	TPTT 1 40K

Tutti i gruppi di continuità in convenzione prevedono una autonomia di batterie minima standard di qualche minuto in caso di mancanza rete. È possibile acquistare espansioni della autonomia per tramite di box batterie atti ad estendere il back-up in caso di mancanza della rete primaria di alimentazione. È estremamente consigliabile installare batterie atte a garantire una autonomia non inferiore ai 30 minuti per consentire la corretta continuità di servizio e la salvaguardia dei dati e dei sistemi alimentati.

Descrizione sintetica:

Serie VIMM da: 1000VA, 1500VA, 2000VA, 3000VA

In fase di sostituzione per End of Sale

Serie GPMM da: 6000VA, 10000VA

Ingresso ed uscita monofase 230Vac, nei range indicati in data sheet

Esecuzione Tower/Rack convertibile

Topologia VFI – On-Line

Cosphi 1

Batterie hot-swap

Funzione Eco-Mode

LCD multifunzione

Onda sinusoidale

Software e scheda di rete inclusi in bundle

Serie TPTM da: 15000VA, 20000VA

Ingresso trifase 380Vac ed uscita monofase 230Vac, nei range indicati in data sheet

Esecuzione Tower

Topologia VFI – On-Line

Cosphi 1

Batterie interne / esterne a seconda dei modelli / autonomia

Funzione Eco-Mode

LCD multifunzione

Onda sinusoidale

Software e scheda di rete inclusi in bundle

Serie TPTT da: 10000VA, 40000VA

Ingresso trifase 380Vac ed uscita trifase 380Vac, nei range indicati in data sheet

Esecuzione Tower

Topologia VFI – On-Line

Cosphi 1

Batterie interne / esterne a seconda dei modelli / autonomia

Funzione Eco-Mode

LCD multifunzione

Onda sinusoidale

Software e scheda di rete inclusi in bundle

SNMP

Model	SNMP Web Card
Protocol Support	TCP/IP, UDP,SNTP, HTTP, DHCP, SNMP v1/2/3,SMTP
UPS Slot Type	Golden Finger
Network Support	RJ45 10/100BaseT
Supported MIB	RFC1213, RFC1628, Vendor MIB
Supported OS	Windows family, Linux and MAC
Supported Extension Devices	Optional environmental monitoring detector
Power Consumption	3 watt (max.)
Operating Temperature	0 ~ 55°C
Operating Humidity	0% ~ 95%
PHYSICAL	
Dimension, D x W x H (mm)	80 x 26 x 52
Net Weight (kgs)	Approx. 0,1 kgs

CAVI DI PARALLELO

Si ricorda che la tecnologia proposta è fornita da PowerMe SRL, azienda italiana, il cui processo è certificato secondo gli standard internazionali:

- Certificazione UNI EN ISO 9001:2015 n. 04-IT-POW-200196 rilasciata da TUV Thuringen Italia S.r.l.
- Certificazione UNI EN ISO 14001:2015 n. 04-IT-POW-210295 rilasciata da TUV Thuringen Italia S.r.l.
- Certificazione ISO 45001:2018 n. 04-IT-POW-210296 rilasciata da TUV Thuringen Italia S.r.l. in data
- Certificazione SA8000:2014 n. 15551 rilasciata da AQSR (American Quality Standards Registrars) Scopo delle certificazioni: Progettazione, produzione, installazione ed assistenza post-vendita di soluzioni software e hardware per accumulo e back-up

PowerMe è, inoltre, iscritta ad Anie Energia ed a garanzia di una corretta gestione dei rifiuti è inoltre iscritta al Ministero dell'Ambiente nelle sezioni:

1. Registro Nazionale Pile ed Accumulatori con numero di iscrizione IT18060P00004828
2. al consorzio RLG, per il trattamento del RAEE secondo quanto previsto dalla normativa vigente in materia di rifiuti. Numero di iscrizione registro AEE IT18090000010777

nel pieno rispetto delle normative vigenti alla data della presente in materia di rifiuti.

Prescrizioni generali di utilizzo

PowerME raccomanda l'utilizzo di soluzioni efficienti dal punto di vista energetico ed a basso impatto ambientale, utilizzate correttamente ed in conformità con le prescrizioni indicate sulle schede tecniche e contenute nei manuali di istruzione. La garanzia è soggetta all'uso corretto dei prodotti, in conformità con le prescrizioni indicate sulle schede tecniche e contenute nei manuali di istruzione.

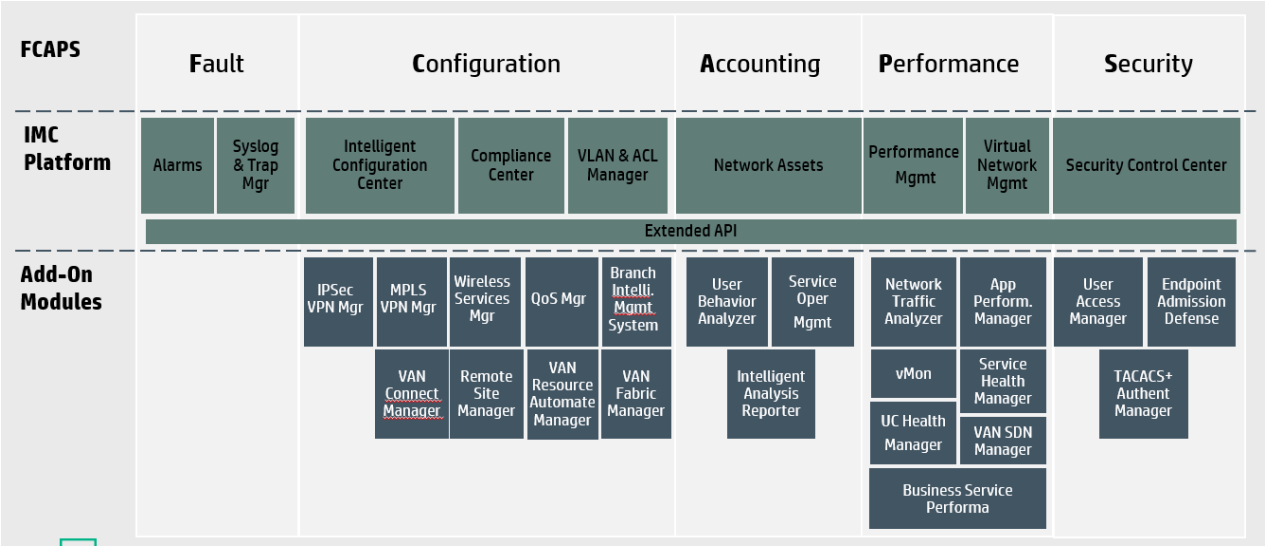
Raccomandazioni

PowerME raccomanda il rispetto delle normative e delle prescrizioni vigenti in materia di idoneità tecnico-professionale e sicurezza sul lavoro in fase di installazione, attivazione e manutenzione delle soluzioni tecnologiche fornite.

6. Piattaforma di gestione e monitoraggio della rete

La piattaforma software HPE Intelligent Management CenterEnterprise è uno strumento per la gestione completa delle reticablate e wireless che supporta il modello FCAPS, forniscegestione aziendale end-to-end dell'IT, scalabilitàdell'architettura di sistema e sistemazione dell'infrastruttura edella nuova tecnologia. La

piattaforma software Intelligent Management Center (IMC) Enterprise supporta la gestione didispositivi sia Hewlett Packard Enterprise che di terze parti. Lalicenza di base inclusa supporta 50 dispositivi, cinque nodi IMC Network Traffic Analyzer, la libreria eAPI e WSM con 50 nodiAP. Licenze aggiuntive sono disponibili per l'acquisto.



Il Modello FCAPS offre i seguenti vantaggi in termini di funzionalità e gestione:

Funzionalità Principali

- Altamente flessibile e scalabile;
- Potente controllo dell'amministrazione;
- Ricca gestione delle risorse;
- Monitoraggio e gestione delle prestazioni dettagliato;
- Reporting centralizzato flessibile.

Gestione

- Modello di implementazione altamente flessibile e scalabile: IMC Standard offre un ampio insieme di funzionalità per la gestione di grandi reti eterogenee; questa soluzione self-contained fornisce scalabilità ed elevata disponibilità attraverso un modello flessibile di distribuzione distribuiti; con il suo design modulare, IMC può essere distribuito attraverso server multipli per fornire una maggiore scalabilità e elasticità
- Identificazione e gestione degli accessi: il sistema implementa una gestione unificata e centralizzata per l'accesso, favorisce l'accesso degli utenti tramite autenticazioni compresi LAN, WAN, WLAN, e VPN, supporta l'autenticazione con smart carta, certificato, supporta varie modalità di controllo degli endpoint e accesso identity-based ai servizi di rete per integrare in modo efficiente la gestione di utenti con risorse e servizi
- Intelligente centro di configurazione: il sistema consente all'amministratore di rete di effettuare la gestione centralizzata dei file di configurazione e file del software, eseguire backup, ripristino e

aggiornamento batch dei file di configurazione, e software / firmware di backup e aggiornamenti, ma anche memorizza e ricerca diverse versioni delle configurazioni dei device e può confrontare e determinare cambiamenti dei file di configurazione

- Gestione delle risorse: il software IMC fornisce uno strumento di discovery degli apparati e della topologia di rete, comprende un inventario dettagliato della rete e rappresentazioni altamente accurate della configurazione; le visualizzazione supportate includono Layer 2 e Layer 3, topologia delle VLAN e la capacità di creare visualizzazioni personalizzate; la personalizzazione consente agli amministratori di organizzare e controllare l'infrastruttura di rete basata sul loro modello organizzativo preferito

La piattaforma software HPE Intelligent Management Center Enterprise è rivolta ad aziende di medie e grandi dimensioni ed è scalabile da centinaia a migliaia di dispositivi. Integra in modo ottimale funzionalità di gestione errori, configurazione elementi e monitoraggio di rete in una singola posizione centralizzata.

La piattaforma software HPE Intelligent Management Center Enterprise offre funzionalità di gestione per una vasta gamma di dispositivi, da router e switch a desktop e server.

Visualizzate e monitorate i dispositivi in un'ampia gamma di metodologie visive, tramite dispositivo, IP, topologia di rete o mediante una visualizzazione personalizzata. Utilizzate il centro di controllo di sicurezza per applicare le impostazioni del dispositivo in modo coerente e allarmi sonori in caso di mancata conformità.

Verificare lo stato di un determinato dispositivo attraverso la pagina dei dettagli dispositivo che contiene riepilogo, test di connettività, dati in tempo reale e la possibilità di utilizzare Telnet/SSH nel dispositivo per risolvere qualsiasi problema.

Sfruttate il centro di configurazione per verificare che i dispositivi siano aggiornati, sottoposti a backup o modificati in qualsiasi modo specifico. Il centro di configurazione può inoltre essere utilizzato per tenere traccia delle modifiche al dispositivo.

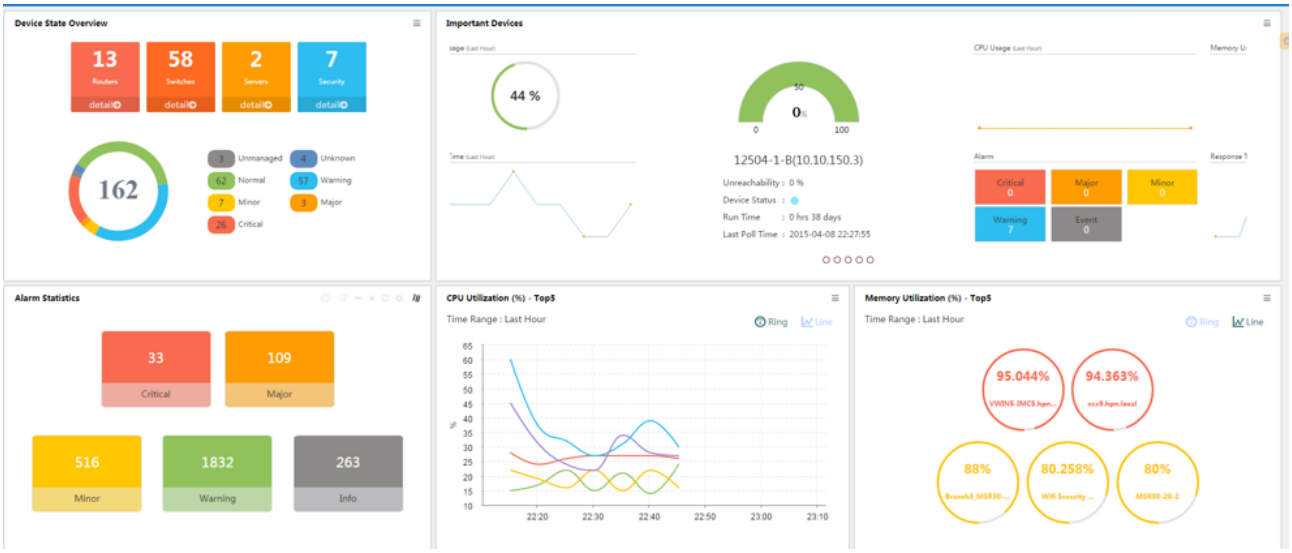
Monitoraggio dettagliato delle prestazioni con notifiche in temporeale

La piattaforma software HPE Intelligent Management Center Enterprise offre la possibilità di monitorare le prestazioni del dispositivo per la generazione di report, le informazioni sulle prestazioni e la notifica di allarmi Monitoraggio singolo o globale dei dispositivi per le impostazioni di soglia che, quando superate, generano un allarme.

Restate all'erta con notifiche di allarme integrato e risolvete facilmente i problemi dalla console o utilizzate un proxy Telnet/SSH.

Include cinque nodi del software IMC Network Traffic Analyzer per l'analisi del traffico di rete e del relativo consumo da parte di diverse applicazioni e utenti.

Comprende 50 nodi del software IMC Wireless Services Manager per analizzare il traffico wireless e fornisce informazioni sull’ambiente wireless della rete.



Gestione della virtualizzazione per VLAN, reti fisiche e virtuali

La piattaforma software HPE Intelligent Management Center Enterprise è uno dei primi strumenti di gestione in grado di integrare e monitorare le reti sia fisiche che virtuali.

Supporta una vasta gamma di hypervisor, tra cui VMware vSphere, MicrosoftHyper-V, Citrix Xen e KVM.

Gestite le VLAN globalmente o in base al dispositivo e create VLAN standardizzate una alla volta o in batch.

Visualizzate lo stato di tutti i VLAN attraverso una visualizzazione della topologia di rete, con la possibilità di monitorare e gestire i dispositivi dalla stessa vista.

L'analisi del traffico sFlow integrata raccoglie le informazioni sul flusso dai dispositivi abilitati, per identificare i colli di bottiglia, riconoscere il traffico anomalo e quantificare i livelli di variazione della larghezza di banda del traffico per applicazioni e servizi diversi. Fornisce una visualizzazione top-down della topologia del traffico.

Effettua il monitoraggio delle prestazioni grazie a TopN, l'analisi delle tendenze, i dati di riepilogo e i display grafici per gli stati dei dispositivi wireless, le statistiche di avviso e il monitoraggio del traffico AP.

All'interno della convenzione, ritroviamo i seguenti pacchetti a seconda del numero di nodi da gestire

SISTEMA	Modello	50 Nodi	100 Nodi	500 Nodi	1000 Nodi
DI MONITORAGGIO E GESTIONE	HPE IMC Std SW Plat E-LTU for Windows and Linux	J-IMC-AAE-AFS			

Le licenze sono cumulabili al fine di fornire una maggiore flessibilità alle amministrazioni, avvicinandosi cosi il più possibile alle esigenze di ognuno.