Cisco Secure Network Analytics

Guida all'installazione dell'appliance hardware serie x2xx (con Data Store)

Sommario

Introduzione **5**

Panoramica 5

Destinatari 6

Come usare la guida 6

Abbreviazioni comuni 7

Considerazioni sulla preconfigurazione **8**

Accesso con la password predefinita CIMC 8

Informazioni sulle appliance Secure Network Analytics 8

Manager 2210 8

Flow Collector 4210 e 5210 9

Data Store 6200 9

Flow Sensor 1210, 3210 e 4240 10

UDP Director 2210 10

Posizionamento delle appliance 10

Posizionamento di Manager 11

Posizionamento del Flow Collector 11

Posizionamento del Flow Sensor 11

Posizionamento di UDP Director 12

Posizionamento di Secure Network Analytics Data Store 13

Porte di comunicazione 14

Integrazione del Flow Sensor nella rete 20

TAP 20

Uso di TAP elettriche 20

Uso di TAP ottiche 21

Uso di TAP esterne al firewall 22

Posizionamento del Flow Sensor all'interno del firewall 22

Porte SPAN 24

Preparazione dell'installazione **26**

Avvertenze relative all'installazione 26
Linee guida per l'installazione 28
Raccomandazioni per la sicurezza 30
Misure di sicurezza per gli interventi su apparecchiature sotto tensione 30
Prevenzione dei danni da scariche elettrostatiche 31
Ambiente del sito 31
Considerazioni sull’alimentazione 32
Considerazioni sulla configurazione del rack 32
Installazione dell'hardware 33
Montaggio dell'appliance 33
Hardware incluso con l'appliance 33
Hardware aggiuntivo richiesto 34
Connessione dell'appliance alla rete 34
Connessione all'appliance 35
Connessione con una tastiera e un monitor 35
Connessione con un laptop 36
Configurazione della rete con la procedura di impostazione iniziale 37
Configurazione generale delle appliance Secure Network Analytics 38
Configurazione dell'indirizzo IP e delle informazioni di gestione dell'appliance 38
Appliance compatibili con il Data Store (Manager 2210, FC 4210) 39
Configurazione della porta di gestione fisica eth0 40
Configurazione dell'indirizzo IP e delle informazioni di gestione dell'appliance 41
Configurazione dell'utilizzo di Data Store 42
Configurazione di Security Analytics and Logging On Prem 43
Configurazione del Data Node 44
Configurazione della porta di gestione fisica eth0 44
Configurazione dell'indirizzo IP e delle informazioni di gestione dell'appliance 46
Configurazione delle porte eth2 ed eth3 per le comunicazioni tra Data Node 47
Modifica della password utente sysadmin 48
Modifica della password sysadmin 48

Modifica della password utente root 49
Modifica della password utente root 49
Configurazione dell'appliance **51**
Contattare il supporto **52**

Introduzione

Panoramica

In questa guida viene illustrato come installare le appliance hardware Cisco Secure Network Analytics serie x2xx (precedentemente Stealthwatch). Vengono descritti i componenti Secure Network Analytics e il modo in cui sono inseriti nel sistema, inclusa l'integrazione con i Flow Sensor. In questa guida vengono descritte anche le operazioni di montaggio e installazione dell'hardware Secure Network Analytics. Componenti hardware della serie x2xx:

Appliance	**Codice prodotto**
Data Store 6200 (tre Data Node)	ST-DS6200-K9 (tre ST-DNODE-G1)
Flow Collector 4210	ST-FC4210-K9
Flow Collector 5210 Engine	ST-FC5210-E
Flow Collector 5210 Database	ST-FC5210-D
Flow Sensor 1210	ST-FS1210-K9
Flow Sensor 3210	ST-FS3210-K9
Flow Sensor 4240	ST-FS4240-K9
Manager 2210 (precedentemente Stealthwatch Management Console)	ST-SMC2210-K9
UDP Director 2210	ST-UDP2210-K9

Destinatari

La presente guida è destinata ai responsabili dell'installazione dei componenti hardware Secure Network Analytics. Inoltre, si presume la conoscenza generale delle procedure di installazione dei dispositivi di rete (Flow Sensor, Flow Collector, UDP Director e Manager).

> Per informazioni sulla configurazione delle appliance Secure Network Analytics, consultare la guida all'installazione e alla configurazione di **Cisco Secure Network Analytics System** e la guida all'implementazione e alla configurazione hardware di Cisco Secure Network Analytics Data Store per la versione software installata. La serie x2xx è compatibile con le versioni software Secure Network Analytics 7.x.

Come usare la guida

Oltre all'introduzione, la guida è divisa nei seguenti capitoli:

Capitolo	Descrizione
2 – **Considerazioni sulla preconfigurazione**	Componenti di Secure Network Analytics, loro posizionamento e configurazione del firewall per le comunicazioni
3 – **Preparazione dell'installazione**	Linee guida, raccomandazioni e avvertenze per la sicurezza
4 – **Installazione dell'hardware**	Montaggio e installazione dei componenti hardware di Secure Network Analytics

Abbreviazioni comuni

Nella guida vengono usate le seguenti abbreviazioni:

Abbreviazione	Descrizione
DMZ	Demilitarized Zone, zona demilitarizzata (una rete perimetrale)
HTTPS	Hypertext Transfer Protocol (Secure), protocollo di trasferimento di un ipertesto
ISE	Identity Services Engine
NIC	Scheda di interfaccia di rete
NTP	Network Time Protocol
PCIe	Peripheral Component Interconnect Express
SNMP	Simple Network Management Protocol
SPAN	Switch Port Analyzer
TAP	Test Access Port
UPS	Uninterruptible Power Supply, gruppo statico di continuità
VLAN	Virtual Local Area Network, LAN virtuale

Considerazioni sulla preconfigurazione

In questa sezione vengono illustrate alcune considerazioni utili per installare e configurare le appliance Secure Network Analytics. Inoltre, viene descritto dove posizionare le appliance Secure Network Analytics e come integrarle nella rete esistente. Include:

- **Accesso con la password predefinita CIMC**
- **Informazioni sulle appliance Secure Network Analytics**
- **Posizionamento delle appliance**
- **Porte di comunicazione**
- **Integrazione del Flow Sensor nella rete**

Accesso con la password predefinita CIMC

Cisco Integrated Management Controller (CIMC) consente l'accesso alla console di configurazione del server, alla console del server virtuale e ai sistemi di monitoraggio dell'integrità dell'hardware.

- Accedere al CIMC come amministratore e digitare la **password** nell'apposito campo.
- Una volta effettuato l'accesso, modificare la password predefinita per garantire una maggiore protezione della rete.

Informazioni sulle appliance Secure Network Analytics

Secure Network Analytics comprende diverse appliance hardware che raccolgono, analizzano e presentano informazioni relative alla rete al fine di migliorarne le prestazioni e la sicurezza. In questa sezione vengono descritte le appliance Secure Network Analytics serie x2xx.

> Per ulteriori informazioni, fare riferimento alle schede tecniche di ciascuna appliance Secure Network Analytics serie x2xx.

Manager 2210

Manager gestisce, coordina, configura e organizza tutti i diversi componenti del sistema. Il software Secure Network Analytics consente di accedere all'interfaccia utente Web della console da qualsiasi computer dotato di accesso a un browser Web. È possibile accedere alle informazioni sulla sicurezza e sulla rete in tempo reale per i segmenti critici dell'azienda. Basata su una piattaforma Java indipendente, Manager offre:

- Gestione, configurazione e reporting centralizzati per un massimo di 25 Secure Network Analytics Flow Collector
- Grafici per la visualizzazione del traffico
- Analisi dettagliate per la risoluzione dei problemi
- Report consolidati e personalizzabili
- Analisi delle tendenze
- Monitoraggio delle prestazioni
- Notifica immediata delle violazioni alla sicurezza

Gli utenti che implementano un Data Store possono configurare un Manager 2210 con un'interfaccia SFP+ DAC a 10 Gbps come eth0 per avere una velocità di trasmissione maggiore. Gli utenti che non implementano un Data Store possono configurare come eth0 solo l'interfaccia in rame da 100 Mbps/1 Gbps/10 Gbps.

Flow Collector 4210 e 5210

Flow Collector raccoglie i dati di NetFlow, cFlow, J-Flow, Packeteer 2, NetStream e IPFIX per proteggere la rete sulla base dei comportamenti.

Flow Collector aggrega i dati sui comportamenti delle reti ad alta velocità provenienti da più reti o segmenti di rete per offrire protezione end-to-end e per migliorare le prestazioni delle reti che coprono diverse aree geografiche.

Gli utenti che implementano un Data Store possono configurare un Flow Collector 4210 con un'interfaccia SFP+ DAC a 10 Gbps come eth0 per avere una velocità di trasmissione maggiore. Gli utenti che non implementano un Data Store possono configurare come eth0 solo l'interfaccia in rame da 100 Mbps/1 Gbps/10 Gbps.

> Mano a mano che riceve i dati, Flow Collector identifica attacchi noti o sconosciuti, uso interno improprio e dispositivi di rete configurati in modo errato, a prescindere dalla crittografia o della frammentazione dei pacchetti. Una volta che Secure Network Analytics ha identificato il comportamento, il sistema può intraprendere l'azione configurata, se disponibile, per quel tipo di comportamento.

Data Store 6200

Il Data Store fornisce un archivio centrale per memorizzare i dati di telemetria della rete raccolti dai Flow Collector. Il Data Store comprende un gruppo di Data Node, ciascuno dei quali contiene una parte dei dati e un backup dei dati di un altro Data Node. Mantenendo tutti i dati in un database centralizzato, anziché averli dispersi su più Flow Collector, il Manager può richiamare i risultati delle query più velocemente dal Data Store anziché

dover interrogare separatamente tutti i Flow Collector. Il gruppo di Data Store offre una migliore tolleranza agli errori, una migliore risposta alle query e permette di popolare i grafici e le tabelle più rapidamente.

Flow Sensor 1210, 3210 e 4240

Flow Sensor è un'appliance di rete che funziona in modo simile a un'appliance di acquisizione di pacchetti tradizionale o IDS, ossia si collega a uno Switch Port Analyzer (SPAN), una porta di mirroring o una porta TAP (Test Access Port) Ethernet. Il Flow Sensor aumenta la visibilità delle seguenti aree di rete:

- Dove non è disponibile NetFlow.
- Dove NetFlow è disponibile, ma si desidera una visibilità più approfondita delle metriche delle prestazioni e dei dati del pacchetto.

Indirizzando il Flow Sensor verso un Flow Collector che supporta NetFlow v9, è possibile ottenere statistiche dettagliate sul traffico. Insieme a Secure Network Analytics Flow Collector, Flow Sensor offre informazioni approfondite sulla metrica delle prestazioni e sugli indicatori comportamentali. Questi indicatori delle prestazioni di flusso offrono informazioni sulla latenza di round-trip introdotta dalla rete o dall'applicazione lato server.

Poiché il Flow Sensor è dotato della visibilità a livello di pacchetto, può calcolare il tempo di round-trip (RTT), il tempo di risposta del server (SRT) e la perdita di pacchetti nelle sessioni TCP. Sono inclusi tutti quei campi nei record NetFlow che vengono inviati al Flow Collector.

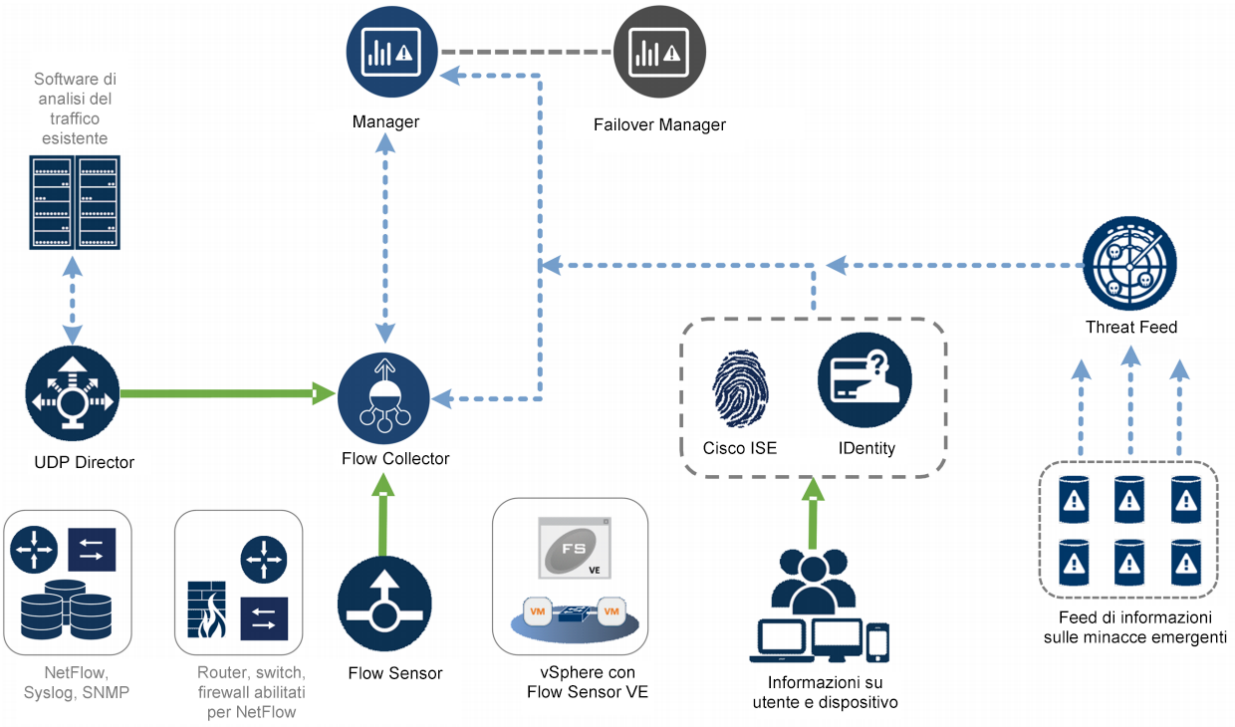
UDP Director 2210

UDP Director consente la replica dei pacchetti UDP ad alta velocità e ad alte prestazioni. L'UDP Director è utile nella ridistribuzione di trap NetFlow, sFlow, syslog o Simple Network Management Protocol (SNMP) a vari collector. Riceve i dati da qualsiasi applicazione UDP senza connessione e poi li ritrasmette a destinazioni diverse, duplicando i dati secondo necessità.

Quando si utilizza la configurazione UDP Director High Availability (HA) (failover), è necessario collegare due appliance UDP Director con cavi crossover. Per istruzioni specifiche, vedere **Connessione dell'appliance alla rete**.

Posizionamento delle appliance

Come mostrato nella figura seguente, è possibile implementare le appliance Secure Network Analytics in modo strategico per fornire una copertura ottimale dei segmenti di rete principali all'interno della rete, sul suo perimetro o nella zona DMZ.



Posizionamento di Manager

In quanto dispositivo di gestione, installare Manager in un punto della rete accessibile da tutti i dispositivi che devono inviare dati.

Se si ha una coppia di Manager per il failover, si consiglia di installare i Manager principale e secondario in punti distinti e separati. Questa strategia consentirà un ripristino di emergenza più facile in caso di necessità.

Posizionamento del Flow Collector

In quanto dispositivo di raccolta e monitoraggio, il Flow Collector deve essere installato in un punto della rete accessibile ai dispositivi NetFlow o sFlow che devono comunicare con il Flow Collector e a tutti i dispositivi che si intende utilizzare per accedere all'interfaccia di gestione degli accessi.

Se si installa un Flow Collector all'esterno del firewall, si raccomanda di disattivare l'impostazione **Accept traffic from any exporter** (Accetta dati da qualsiasi esportatore).

Posizionamento del Flow Sensor

In quanto dispositivo di monitoraggio passivo, il Flow Sensor può essere collocato in molteplici punti della rete per osservare e registrare le attività IP e di conseguenza proteggere l'integrità della rete e rilevare eventuali violazioni della sicurezza. Il Flow

Sensor contiene sistemi di gestione integrati basati sul Web che facilitano la gestione centralizzata o remota e l'amministrazione.

L'appliance Flow Sensor è più efficace se posizionata nei segmenti critici della rete aziendale, come indicato di seguito:

- All'interno del firewall per monitorare il traffico e stabilire se si è verificata una violazione di firewall
- All'esterno del firewall per monitorare il flusso di traffico che minaccia il firewall
- In segmenti sensibili della rete, per garantire la protezione da dipendenti insoddisfatti o hacker con accesso root
- In punti remoti che costituiscono le estensioni vulnerabili della rete
- Nella rete aziendale per la gestione dei protocolli (ad esempio, sulla subnet dei servizi di transazione per stabilire se un hacker è in esecuzione su Telnet o FTP e può compromettere i dati finanziari dei clienti)

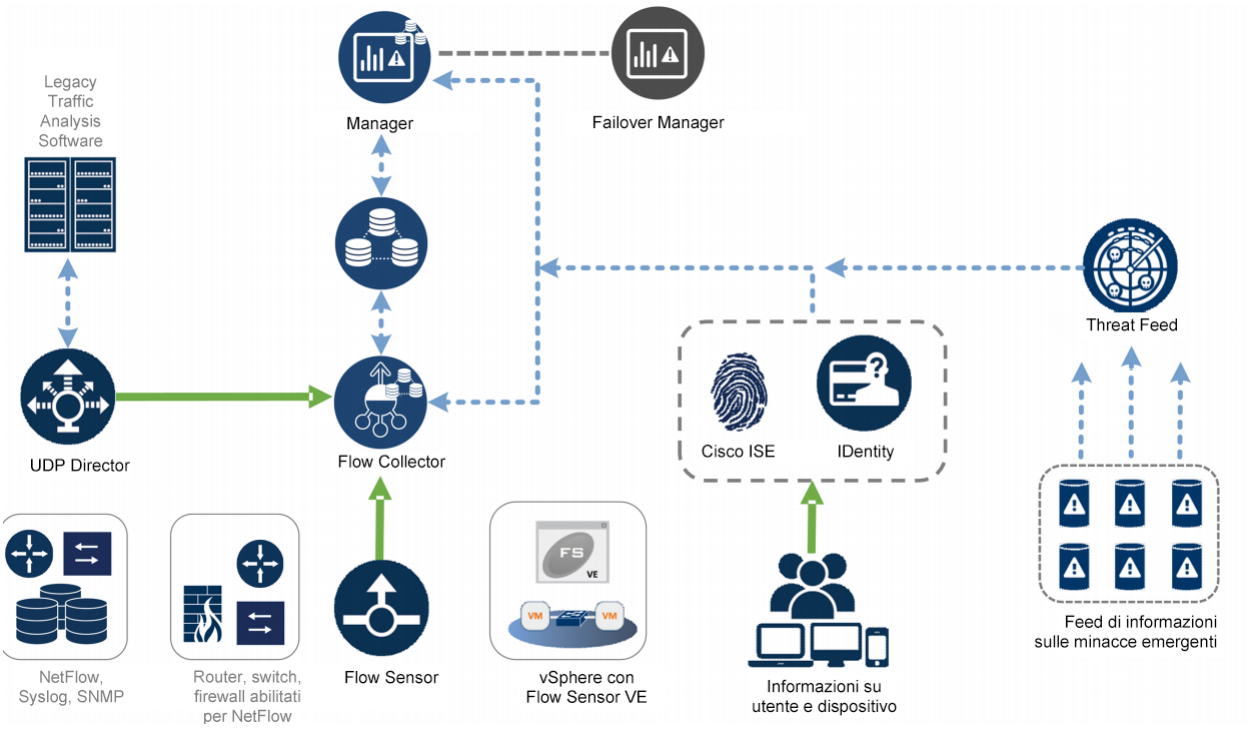
Posizionamento di UDP Director

L'unico requisito per il posizionamento di UDP Director è assicurare un percorso di comunicazione senza ostacoli con il resto delle appliance Secure Network Analytics.

Se UDP Director deve essere implementato in un ambiente con ACI Cisco e con il controllo Unicast Reverse Path Forwarding (uRPF) abilitato o l'opzione **Limit IP learning to subnet** (Limita apprendimento IP sulla subnet) abilitata, la rete locale potrebbe bloccare il traffico inoltrato da UDP Director. Per permettere agli strumenti di raccolta dati di sapere da dove origina il traffico, è necessario specificare lo spoofing del traffico UDP nelle regole di inoltro.

In questo caso, per garantire un corretto funzionamento, implementare UDP Director su un segmento della rete dove è possibile disabilitare il controllo uRPF o l'opzione **Limit IP learning to subnet** (in genere un segmento interno). È possibile posizionare UDP Director in un'uscita L3 (senza apprendimento IP). Sulle versioni 4.0 e superiori, è possibile disabilitare l'apprendimento degli endpoint su ciascun VRF.

Il diagramma seguente mostra un'implementazione di Secure Network Analytics con un Data Store.

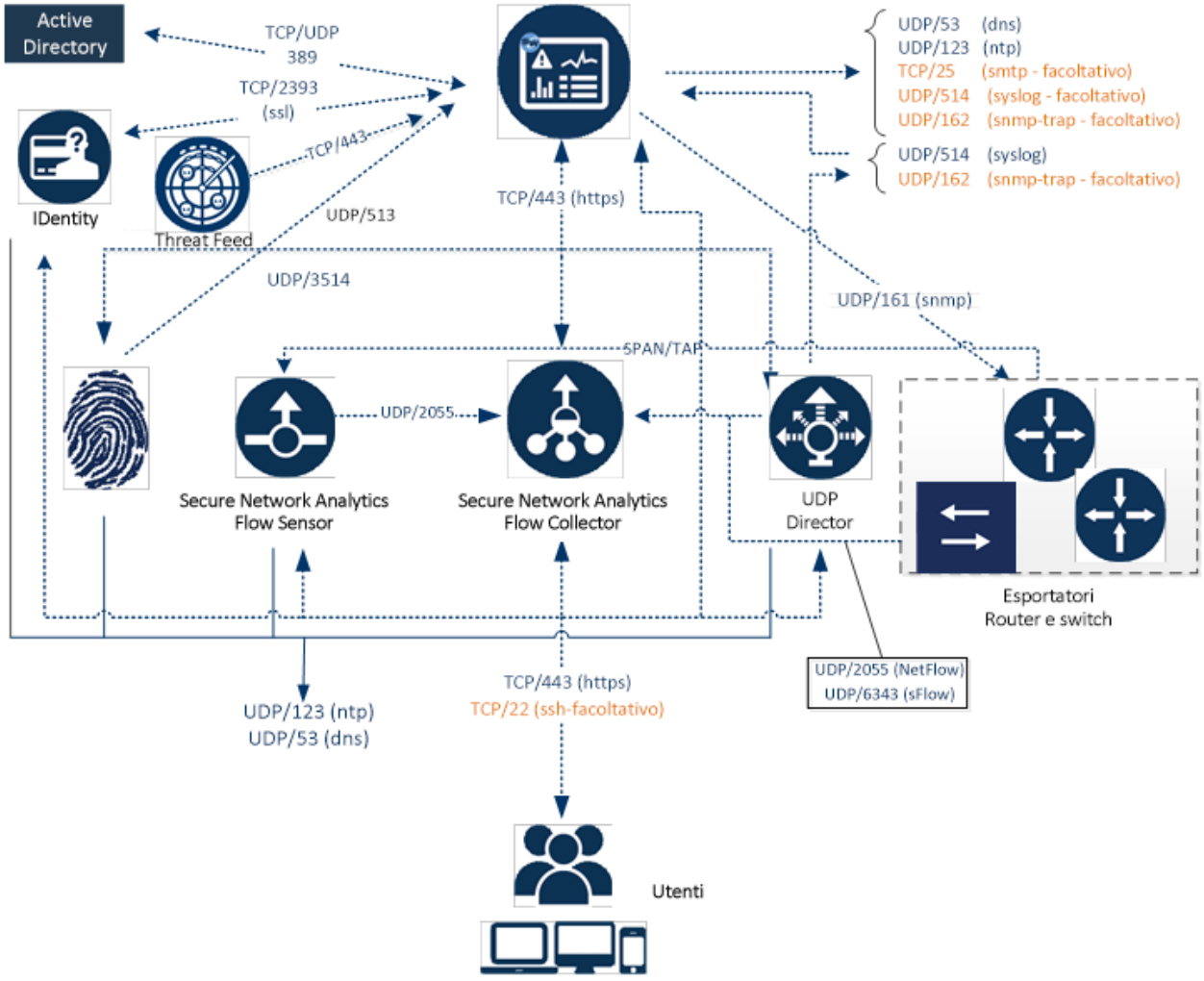


Posizionamento di Secure Network Analytics Data Store

Come archivio dei dati raccolti dai Flow Collector e come archivio centralizzato interrogato da un Manager, installare i Data Node in una posizione della rete accessibile a tutti i Flow Collector e al Manager. Per ulteriori informazioni, vedere la guida all'implementazione e alla configurazione hardware del Data Store.

Porte di comunicazione

Il diagramma seguente mostra le porte di comunicazione da aprire durante l'implementazione di Secure Network Analytics.



Nella tabella seguente viene mostrato l'uso delle porte in Secure Network Analytics:

Da (Client)	A (Server)	Porta	Protocollo
PC utente amministratore	Tutte le appliance	TCP/443	HTTPS
Tutte le appliance	Origine ora rete	UDP/123	NTP
Active Directory	Manager	TCP/389, UDP/389	LDAP

Da (Client)	A (Server)	Porta	Protocollo
Cisco ISE	Manager	TCP/443	HTTPS
Cisco ISE	Manager	TCP/8910	XMPP
Origini log esterni	Manager	UDP/514	SYSLOG
Flow Collector	Manager	TCP/443	HTTPS
Threat Feed	Manager	TCP/443 o connessione tramite proxy	HTTPS
UDP Director	Flow Collector – sFlow	UDP/6343	sFlow
UDP Director	Flow Collector – NetFlow	UDP/2055*	NetFlow
UDP Director	Sistemi di gestione eventi di terze parti	UDP/514	SYSLOG
Flow Sensor	Manager	TCP/443	HTTPS
Flow Sensor	Flow Collector – NetFlow	UDP/2055	NetFlow
Identity	Manager	TCP/2393	SSL
Esportatori NetFlow	Flow Collector – NetFlow	UDP/2055*	NetFlow
Esportatori sFlow	Flow Collector – sFlow	UDP/6343*	sFlow
Manager	Cisco ISE	TCP/443	HTTPS
Manager	DNS	UDP/53	DNS
Manager	Flow Collector	TCP/443	HTTPS
Manager	Flow Sensor	TCP/443	HTTPS
Manager	Identity	TCP/2393	SSL

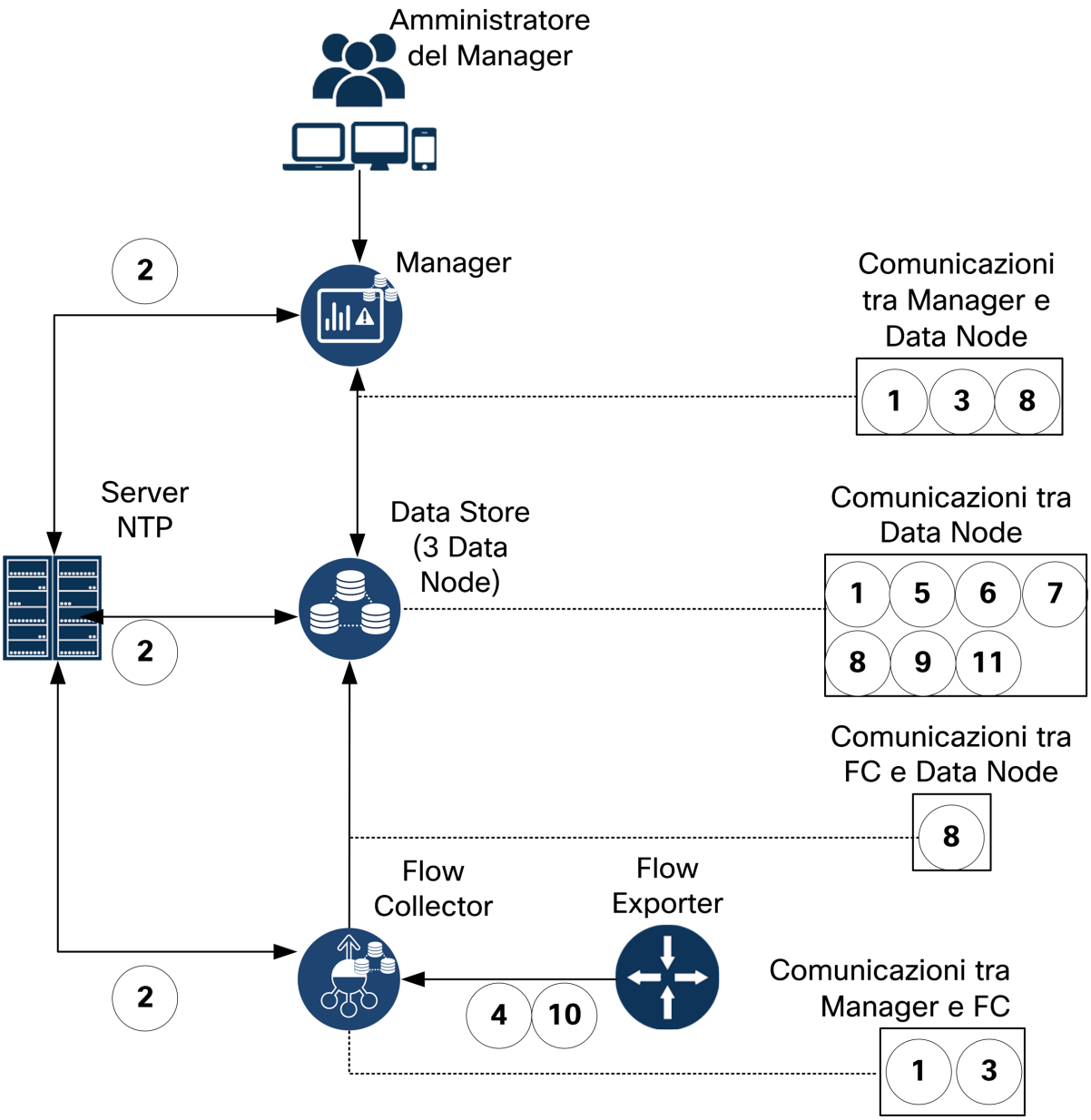
Da (Client)	A (Server)	Porta	Protocollo
Manager	Esportatori di flussi	UDP/161	SNMP
PC utente	Manager	TCP/443	HTTPS

*Questa è la porta predefinita, ma è possibile configurare qualsiasi porta UDP sull'esportatore.

La seguente tabella è dedicata alle configurazioni facoltative disponibili a seconda delle esigenze di gestione della rete:

Da (Client)	A (Server)	Porta	Protocollo
Tutte le appliance	PC utente	TCP/22	SSH
Manager	Gestione eventi di terze parti	UDP/162	Trap SNMP
Manager	Gestione eventi di terze parti	UDP/514	SYSLOG
Manager	Gateway e-mail	TCP/25	SMTP
Manager	Threat Feed	TCP/443	SSL
PC utente	Tutte le appliance	TCP/22	SSH

Nel diagramma seguente vengono mostrate le porte aggiuntive da aprire per l'implementazione di un Data Store sulla rete:



Nella tabella seguente sono indicate le porte utilizzate per implementare un Data Store sulla rete:

N°	Da (Client)	A (Server)	Porta	Protocollo o scopo
1	Manager	Flow Collector e Data Node	22/TCP	SSH, necessario per inizializzare il database del Data Store

1	Data Node	Tutti gli altri Data Node	22/TCP	SSH, necessario per inizializzare il database del Data Store e per le attività di amministrazione del database
2	Manager, Flow Collector e Data Node	Server NTP	123/UDP	NTP, richiesto per la sincronizzazione dell'ora
2	Server NTP	Manager, Flow Collector e Data Node	123/UDP	NTP, richiesto per la sincronizzazione dell'ora
3	Manager	Flow Collector e Data Node	443/TCP	HTTPS, necessario per comunicazioni sicure tra le appliance
3	Flow Collector	Manager	443/TCP	HTTPS, necessario per comunicazioni sicure tra le appliance
3	Data Node	Manager	443/TCP	HTTPS, necessario per comunicazioni sicure tra le appliance
4	Esportatori NetFlow	Flow Collector (NetFlow)	2055/UDP	Inserimento NetFlow
5	Data Node	Tutti gli altri Data Node	4803/TCP	Servizio di messaggistica tra Data Node
6	Data Node	Tutti gli altri Data Node	4803/UDP	Servizio di messaggistica tra Data Node
7	Data Node	Tutti gli altri Data Node	4804/UDP	Servizio di messaggistica tra Data Node

8	Manager, Flow Collector e Data Node	Data Node	5433/TCP	Connessioni client Vertica
9	Data Node	Tutti gli altri Data Node	5433/UDP	Monitoraggio del servizio di messaggistica Vertica
10	Esportatori sFlow	Flow Collector (sFlow)	6343/UDP	Inserimento sFlow
11	Data Node	Tutti gli altri Data Node	6543/UDP	Servizio di messaggistica tra Data Node

Integrazione del Flow Sensor nella rete

Il Flow Sensor è estremamente versatile e può essere integrato in un'ampia gamma di topologie, tecnologie e componenti di rete. Sebbene in questa sede non vengano descritte tutte le configurazioni di rete, gli esempi riportati possono aiutare nella scelta della migliore impostazione per le proprie esigenze.

Prima di installare un Flow Sensor, è necessario prendere alcune decisioni sulla rete e su come si desidera monitorarla. Analizzare la topologia della rete e le esigenze di monitoraggio specifiche. Si consiglia di connettere un Flow Sensor in modo che riceva le trasmissioni di rete da e verso la rete monitorata e, se lo si desidera, riceva anche le trasmissioni di rete interne.

Nelle seguenti sezioni viene descritto come integrare un'appliance Flow Sensor nella rete utilizzando i seguenti dispositivi di rete Ethernet:

- **TAP**
- **Porte SPAN**

TAP

Quando una Test Access Port (TAP) viene posizionata in linea con una connessione di rete, ripete la connessione su una o più porte separate. Ad esempio, una TAP Ethernet installata in linea con un cavo Ethernet trasmetterà nuovamente i dati in ciascuna direzione su porte separate. Pertanto, usare una TAP è il modo più affidabile per utilizzare il Flow Sensor. Il tipo di TAP da utilizzare dipende dalla rete.

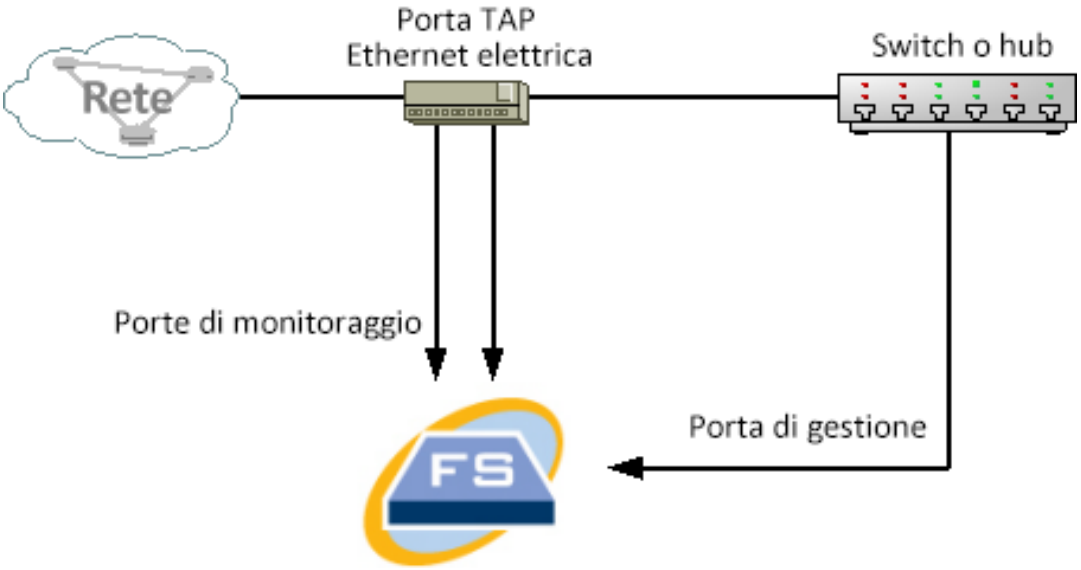
In questa sezione vengono descritti i metodi di utilizzo delle TAP:

- **Uso di TAP elettriche**
- **Uso di TAP ottiche**
- **Uso di TAP esterne al firewall**
- **Posizionamento del Flow Sensor all'interno del firewall**

In una rete con TAP, il Flow Sensor può catturare i dati di monitoraggio delle prestazioni solo se è connesso a una TAP di aggregazione, ossia in grado di acquisire sia il traffico in entrata che in uscita. Se il Flow Sensor è connesso a una TAP unidirezionale, ossia in grado di acquisire solo il traffico in una direzione su ciascuna porta, il Flow Sensor non catturerà i dati di monitoraggio delle prestazioni.

Uso di TAP elettriche

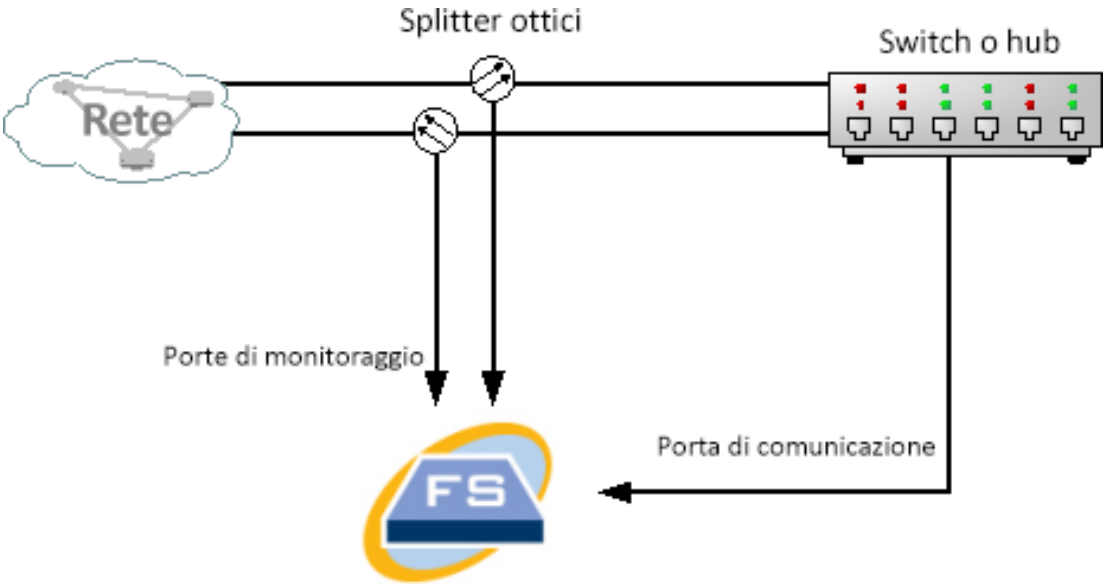
Nell'esempio seguente, il Flow Sensor è connesso a una TAP Ethernet elettrica. Per effettuare questa configurazione, connettere due porte TAP alle porte di monitoraggio 1 e 2 del Flow Sensor.



Uso di TAP ottiche

Utilizzare due splitter per sistemi a fibra ottica. Posizionare uno splitter per cavo in fibra ottica in linea con ciascuna direzione di trasmissione per ripetere il segnale ottico in una direzione.

Nell'esempio seguente, il Flow Sensor è connesso alla rete basata su fibra ottica. Per effettuare questa configurazione, connettere le uscite degli splitter alle porte di monitoraggio 1 e 2 del Flow Sensor.



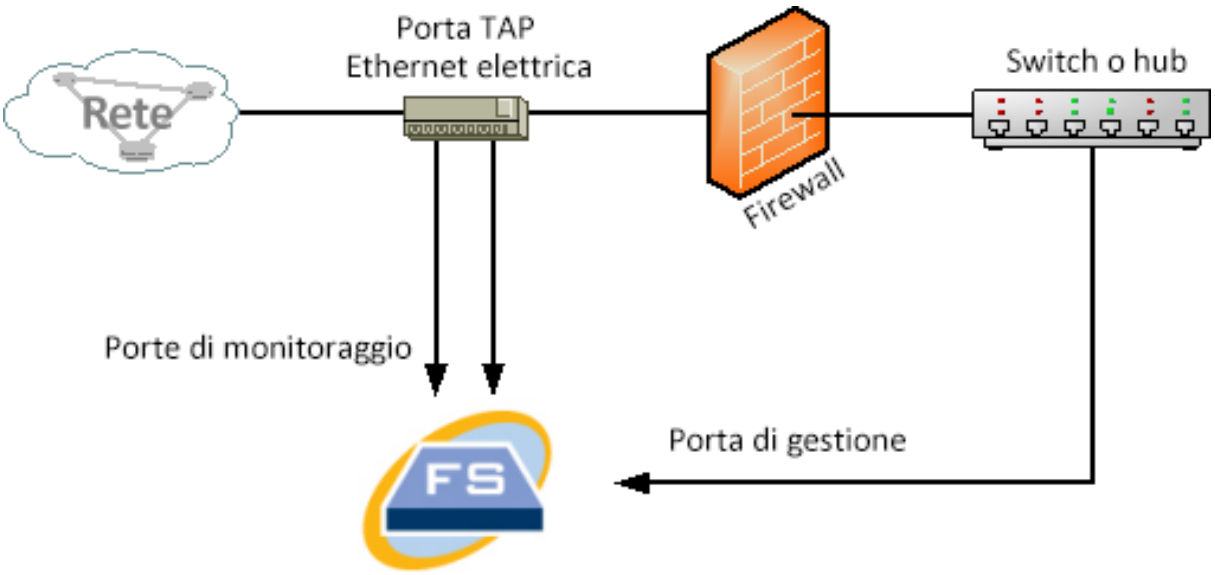
Se la connessione tra le reti monitorate è una connessione ottica, il Flow Sensor è connesso a due splitter ottici. La porta di gestione è connessa allo switch della rete monitorata o a un altro switch o hub.

Uso di TAP esterne al firewall

Affinché il Flow Sensor monitori il traffico tra il firewall e le altre reti, collegare la porta di gestione Secure Network Analytics a uno switch o una porta esterna al firewall.

Si raccomanda di utilizzare una TAP per questa connessione in modo che un eventuale guasto del dispositivo non danneggi l'intera rete.

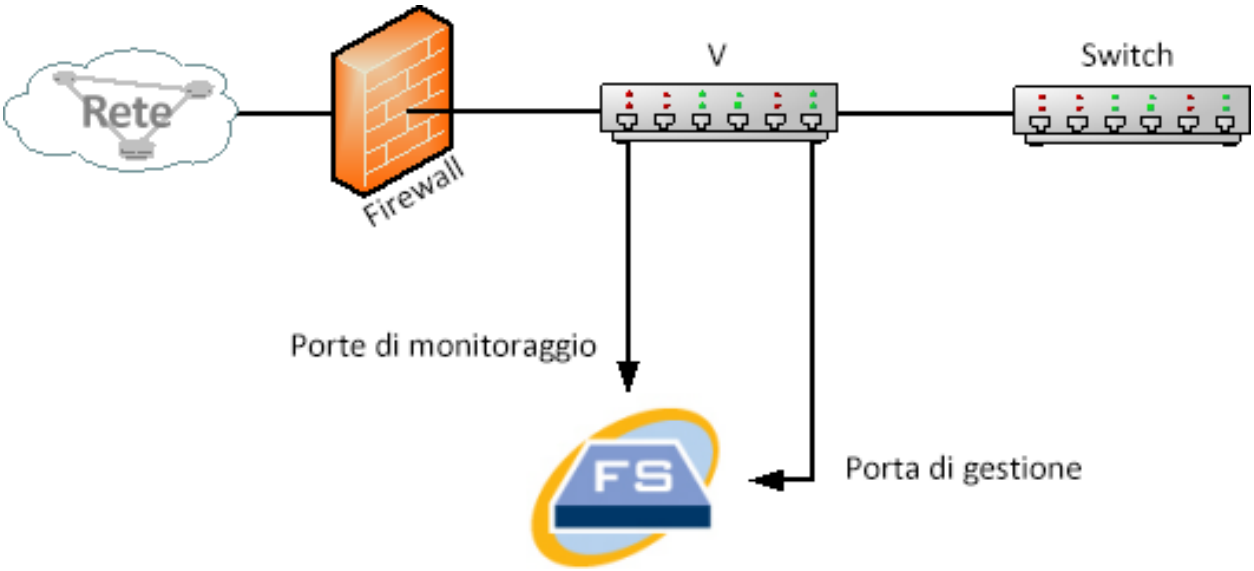
Nell'esempio riportato di seguito viene illustrato l'uso di una TAP Ethernet elettrica. La porta di gestione deve essere connessa allo switch o all'hub della rete monitorata. Questa configurazione è simile a quella che prevede il monitoraggio del traffico da e verso la rete.



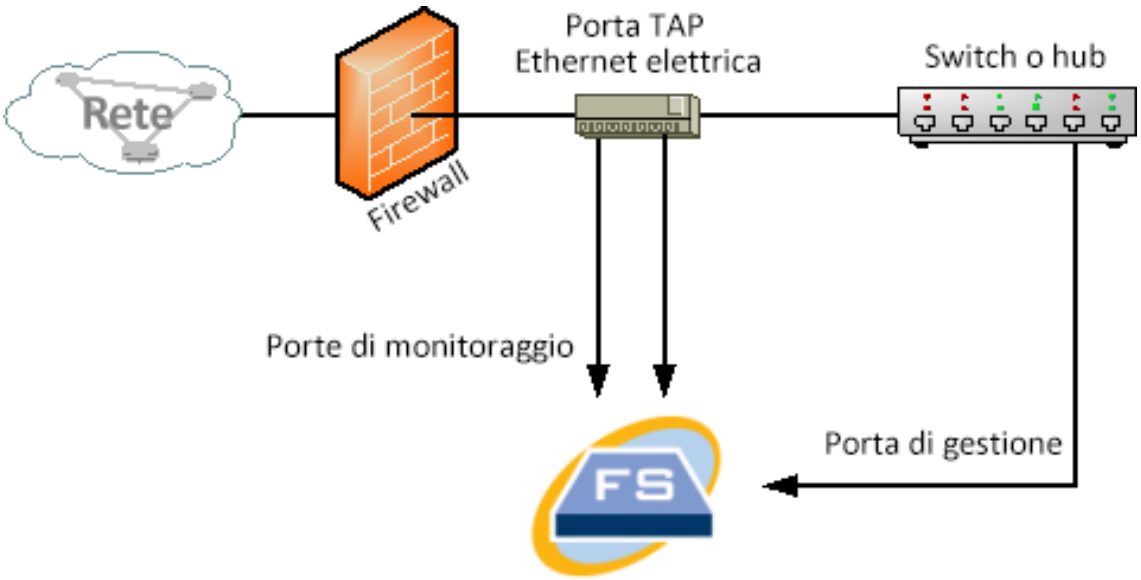
Se il firewall esegue la NAT (Network Address Translation), è possibile osservare solo gli indirizzi presenti sul firewall.

Posizionamento del Flow Sensor all'interno del firewall

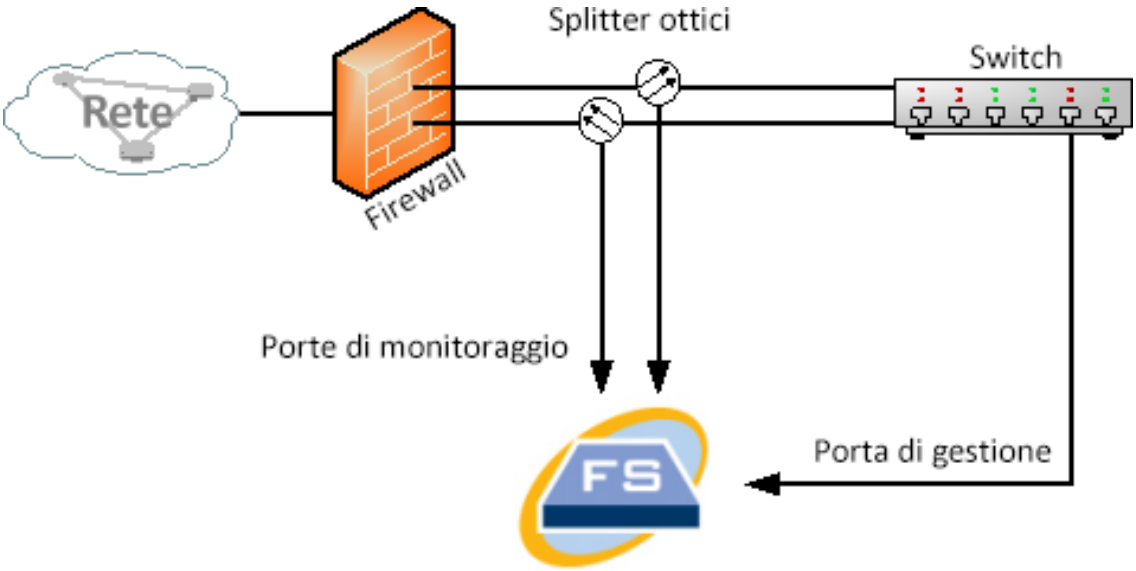
Per monitorare il traffico tra reti interne e firewall, il Flow Sensor deve essere in grado di accedere a tutto il traffico tra il firewall e le reti interne. Per ottenere questo risultato, è necessario configurare una porta di mirroring che rifletta la connessione al firewall sullo switch principale. Assicurarsi che la porta di monitoraggio 1 del Flow Sensor sia connessa alla porta di mirroring, come mostrato nella figura riportata di seguito:



Per monitorare il traffico all'interno del firewall con una TAP, inserire la TAP o lo splitter ottico tra il firewall e lo switch principale o hub. Di seguito viene illustrata una configurazione con una TAP.



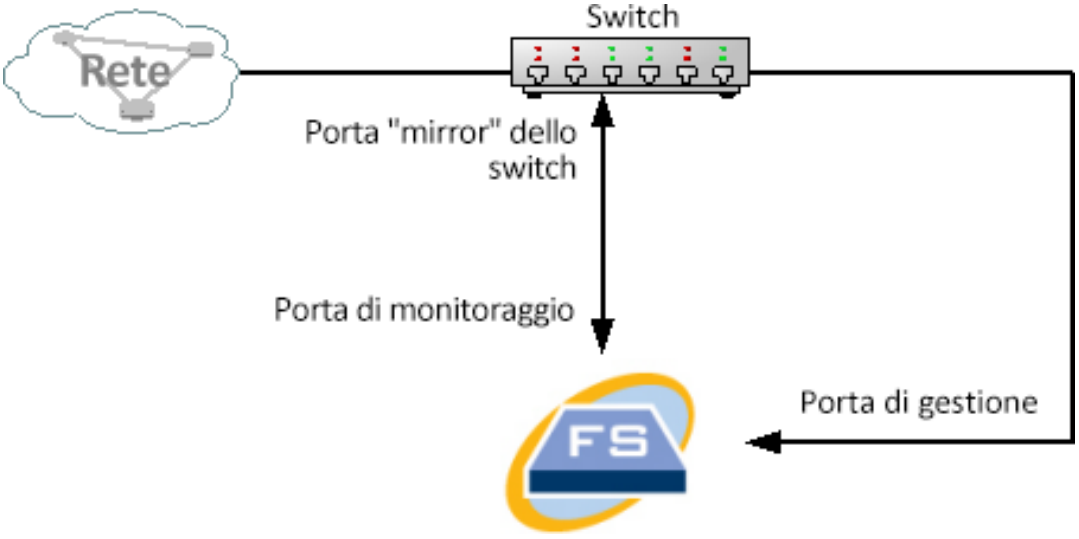
Di seguito viene illustrata una configurazione con splitter ottico.



Porte SPAN

Il Flow Sensor può essere collegato anche a uno switch. Tuttavia, poiché uno switch non ripete tutto il traffico su ogni porta, il Flow Sensor non funzionerà correttamente a meno che lo switch non trasmette nuovamente i pacchetti ricevuti e inviati da una o più porte dello switch. Questo tipo di porta dello switch è talvolta denominato porta di mirroring o Switch Port Analyzer (SPAN).

La figura seguente mostra in che modo è possibile ottenere questa configurazione collegando la rete a Secure Network Analytics Flow Sensor tramite la porta di gestione.



In questo caso è necessario configurare una porta dello switch (denominata anche porta di mirroring) per ripetere tutto il traffico inviato e ricevuto dall'host interessato sulla porta di mirroring. La porta di monitoraggio 1 del Flow Sensor deve essere connessa a questa porta di mirroring. In questo modo il Flow Sensor può monitorare il traffico inviato e ricevuto dalla rete interessata e da altre reti. In questo caso, una rete può essere composta da alcuni o da tutti gli host collegati allo switch.

Un modo comune di configurare le reti su uno switch consiste nel suddividerle in reti virtuali (VLAN, Virtual Local Area Network), ossia con connessioni di host logiche anziché fisiche. Se la porta di mirroring è configurata per riflettere tutte le porte su una VLAN o uno switch, il Flow Sensor può monitorare tutto il traffico inviato e ricevuto dalla rete interessata, all'interno della rete stessa e di altre reti.

In tutti i casi, si consiglia di consultare la documentazione del produttore dello switch per stabilire come configurare la porta di mirroring dello switch e quale traffico ripetere per la porta di mirroring.

Preparazione dell'installazione

Avvertenze relative all'installazione

Prima di installare le appliance Secure Network Analytics serie x2xx, leggere il documento con le informazioni sulla conformità alle normative e sulla sicurezza.

Osservare quanto segue:

Avvertenza 1071: definizione delle avvertenze

ISTRUZIONI IMPORTANTI SULLA SICUREZZA

Questo simbolo di avvertenza indica un pericolo. La situazione potrebbe causare infortuni alle persone. Prima di utilizzare qualsiasi apparecchiatura, occorre essere al corrente dei pericoli relativi ai circuiti elettrici e conoscere le procedure standard per la prevenzione di incidenti. Utilizzare il numero presente alla fine di ciascuna avvertenza per individuare le traduzioni delle avvertenze fornite con il dispositivo.

CONSERVARE QUESTE ISTRUZIONI

Avvertenza 1005: interruttore automatico

Questo prodotto dipende dall'impianto dell'edificio per quanto riguarda la protezione da cortocircuiti (sovracorrente). Assicurarsi che il dispositivo di protezione non abbia una classe superiore a 120 V, 15 A per gli Stati Uniti (250 V, 16 A per l'Unione europea).

Avvertenza 1004: istruzioni per l’installazione

Leggere le istruzioni per l'installazione prima di usare, montare o collegare il sistema all'alimentazione.

Avvertenza 12: avvertenza sulla disconnessione dell’alimentazione

Prima di intervenire su uno chassis o di lavorare vicino agli alimentatori, scollegare il cavo di alimentazione sulle unità CA; scollegare l'alimentazione all’interruttore automatico sulle unità CC.

Avvertenza 43: avvertenza per la rimozione degli oggetti preziosi

Prima di utilizzare apparecchiature collegate alle linee elettriche, rimuovere eventuali gioielli e accessori in metallo (anelli, collane e orologi) indossati. Poiché gli oggetti metallici si riscaldano se collegati all'alimentazione e alla messa a terra, si rischia di subire gravi ustioni oppure l'oggetto stesso può saldarsi ai terminali.

Avvertenza 94: avvertenza sul bracciale antistatico

Durante questa procedura, indossare il bracciale antistatico per la messa a terra in modo da evitare danni alla scheda dovuti a scariche elettrostatiche. Non toccare direttamente con la mano o con strumenti metallici il backplane per evitare il rischio di scosse elettriche.

Avvertenza 1045: protezione da cortocircuiti

Per questo prodotto è necessario predisporre la protezione contro i cortocircuiti (sovracorrente) nell'ambito dell'impianto dell'edificio. Installare solo in conformità con le normative nazionali e locali che regolano il cablaggio.

Avvertenza 1021: circuito SELV

Per evitare shock elettrici, non collegare i circuiti a bassissima tensione di sicurezza (SELV) ai circuiti telefonici (TNV). Le porte LAN includono circuiti SELV, mentre le porte WAN utilizzano circuiti TNV. Alcune porte LAN e WAN utilizzano connettori RJ-45. Prestare attenzione durante il collegamento dei cavi.

Avvertenza 1024: conduttore di messa a terra

Questa apparecchiatura deve essere dotata di messa a terra. Non escludere mai il conduttore di protezione né usare l'apparecchiatura in assenza di un conduttore di protezione installato in modo corretto. Se non si è certi della disponibilità di un adeguato collegamento di messa a terra, richiedere un controllo alle autorità competenti o rivolgersi a un elettricista.

Avvertenza 1040: smaltimento del prodotto

Il prodotto deve essere smaltito in ottemperanza alle normative nazionali vigenti.

Avvertenza 1074: conformità alle normative elettriche locali e nazionali

L'installazione dell'apparecchiatura deve essere conforme alle normative elettriche locali e nazionali.

Avvertenza 19: avviso di alimentazione TN

Il dispositivo è progettato per funzionare con sistemi elettrici TN.

Linee guida per l'installazione

Osservare quanto segue:

Avvertenza 1047: prevenzione del surriscaldamento

Per evitare che il sistema si surriscaldi, non utilizzarlo in un'area in cui la temperatura ambiente è superiore alla temperatura massima consigliata di 5 – 35 °C (41 – 95 °F)

Avvertenza 1019: dispositivo di scollegamento principale

Il gruppo spina-presa deve essere sempre accessibile in quanto serve da sistema di disconnessione principale.

Avvertenza 1005: interruttore automatico

Questo prodotto dipende dall'impianto dell'edificio per quanto riguarda la protezione da cortocircuiti (sovracorrente). Assicurarsi che il dispositivo di protezione non abbia una classe superiore a 120 V, 15 A per gli Stati Uniti (250 V, 16 A per l'Unione europea).

Avvertenza 1074: conformità alle normative elettriche locali e nazionali

L'installazione dell'apparecchiatura deve essere conforme alle normative elettriche locali e nazionali.

Dichiarazione 371: cavo di alimentazione e adattatore CA

Per l'installazione del prodotto, utilizzare i cavi di collegamento, i cavi di alimentazione, gli adattatori CA e le batterie in dotazione o indicati nelle istruzioni. Se si dovessero usare cavi o adattatori diversi, potrebbero verificarsi guasti e incendi. Le norme giapponesi in materia di sicurezza dei materiali e degli apparecchi elettrici vietano l'utilizzo di cavi con certificazione UL (sui quali è riportato il marchio UL o CSA), in quanto non disciplinati dalle disposizioni di legge che prevedono invece il marchio PSE sul cavo, per tutti i dispositivi elettrici diversi da quelli indicati da CISCO.

Avvertenza 1073: nessun componente soggetto a manutenzione da parte dell'utente

Non vi sono all'interno componenti soggetti a manutenzione da parte dell'utente. Non aprire.

Per l'installazione di uno chassis, adottare le seguenti linee guida:

- Assicurarsi che vi sia spazio sufficiente intorno allo chassis per consentire la manutenzione e un flusso d'aria adeguato. L'aria nello chassis fluisce dalla parte anteriore a quella posteriore.

  Per garantire un corretto flusso d'aria è necessario montare lo chassis in rack per mezzo dei kit guide. Se le unità vengono installate una sopra all'altra o impilate senza kit guide, le prese d'aria sulla parte superiore dello chassis vengono ostruite causando il surriscaldamento, l'aumento di velocità delle ventole e un maggiore consumo energetico. Si consiglia di montare lo chassis in rack con kit guide in quanto queste offrono la distanza minima richiesta. L'uso dei kit guide per il montaggio dello chassis non richiede l'uso di distanziatori aggiuntivi.

- Verificare che il climatizzatore possa mantenere lo chassis a una temperatura di 5 – 35 °C (41 – 95 °F).
- Assicurarsi che il rack o l'armadio soddisfi i requisiti di montaggio in rack.
- Assicurarsi che l'alimentazione del sito sia conforme ai requisiti indicati nella scheda tecnica dell'appliance. Se disponibile, è possibile utilizzare un UPS come protezione da possibili guasti nell'alimentazione.

> Evitare i tipi di UPS che utilizzano tecnologia ferro-risonante. Questi tipi di UPS possono diventare instabili con questi sistemi, che possono avere fluttuazioni notevoli in termini di assorbimento di corrente a causa di pattern di traffico dati oscillanti.

Raccomandazioni per la sicurezza

Utilizzare le seguenti informazioni per garantire la propria sicurezza e proteggere lo chassis. Queste informazioni potrebbero non comprendere tutte le situazioni potenzialmente rischiose nell'ambiente di lavoro, quindi prestare attenzione e prendere sempre decisioni ponderate.

Osservare queste linee guida sulla sicurezza:

- Mantenere l'area pulita e priva di polvere prima, durante e dopo l'installazione.
- Tenere gli strumenti lontani dalle aree di passaggio per evitare che qualcuno possa inciamparvi.
- Non indossare abiti molto larghi o gioielli, come orecchini, braccialetti o collane, che potrebbero restare impigliati nello chassis.
- Indossare gli occhiali protettivi se le condizioni di lavoro potrebbero essere pericolose per gli occhi.
- Non compiere azioni che possono generare eventuali pericoli per le persone o rendere l'apparecchiatura pericolosa.
- Non tentare mai di sollevare un oggetto troppo pesante per una persona sola.

Misure di sicurezza per gli interventi su apparecchiature sotto tensione

> Prima di intervenire su uno chassis, assicurarsi che il cavo di alimentazione sia scollegato.

Quando si utilizzano apparecchiature con alimentazione elettrica, attenersi alle seguenti linee guida:

- Non lavorare da soli se sussistono condizioni di potenziale pericolo nella propria area di lavoro.
- Non dare per scontato che l'alimentazione sia scollegata; controllare sempre.

- Verificare attentamente la presenza di eventuali pericoli nell'area di lavoro, ad esempio superfici bagnate, prolunghe di alimentazione senza messa a terra, cavi di alimentazione consumati e assenza di messa a terra.
- In caso di incidente elettrico:
    - Agire con cautela per evitare di subire danni.
    - Scollegare l'alimentazione dal sistema.
    - Se possibile, mandare un'altra persona a chiamare il soccorso medico. Altrimenti, valutare le condizioni della vittima e chiedere aiuto.
    - Stabilire se è necessario praticare la respirazione bocca a bocca o il massaggio cardiaco, quindi intervenire in maniera adeguata.
- Utilizzare lo chassis rispettando le specifiche elettriche indicate e le istruzioni per l'uso del prodotto.

Prevenzione dei danni da scariche elettrostatiche

Le scariche elettrostatiche si verificano quando i componenti elettronici vengono gestiti in modo improprio. Possono danneggiare l'apparecchiatura e compromettere i circuiti elettrici, causando il guasto sporadico o definitivo dell'apparecchiatura.

Attenersi sempre alle procedure di prevenzione delle scariche elettrostatiche quando si rimuovono o si sostituiscono i componenti. Verificare che lo chassis sia collegato alla messa a terra. Indossare un bracciale antistatico, controllando che aderisca alla pelle. Collegare il morsetto della messa a terra a una parte non verniciata del telaio dello chassis in modo da scaricare a terra le tensioni elettrostatiche in totale sicurezza. Per evitare danni e shock elettrostatici, utilizzare il bracciale e il cavo in modo corretto. Se non è disponibile un bracciale antistatico, toccare la parte in metallo dello chassis per scaricare a terra l'eventuale elettricità statica accumulata.

Per operare in sicurezza, controllare periodicamente che il valore di resistenza del bracciale antistatico sia compreso tra 1 e 10 megaohm.

Ambiente del sito

Per evitare guasti alle apparecchiature e ridurre la possibilità di arresti causati da condizioni ambientali, pianificare la disposizione del sito e il posizionamento delle apparecchiature. In caso di arresto o di un numero insolitamente elevato di errori delle apparecchiature esistenti, queste considerazioni possono servire per individuarne la causa ed evitare problemi futuri.

Considerazioni sull’alimentazione

Quando si installa lo chassis, tenere in considerazione quanto segue:

- Controllare l'alimentazione prima di installare lo chassis per assicurarsi che la sede di installazione sia priva di picchi di corrente e interferenze. Installare uno stabilizzatore di tensione, se necessario, per garantire i voltaggi e i livelli di alimentazione adeguati nella tensione di ingresso dell’appliance.
- Installare la messa a terra adeguata per la sede in modo da evitare danni derivati da fulmini e sbalzi di corrente.
- Lo chassis non ha un intervallo operativo selezionabile dall’utente. Fare riferimento all'etichetta sullo chassis per i corretti requisiti di alimentazione in ingresso dell’appliance.
- Sono disponibili diversi tipi di cavi di alimentazione in ingresso CA per l'appliance; assicurarsi di disporre del tipo corretto per il proprio impianto.
- In caso di utilizzo di alimentatori doppi ridondanti (1+1), si consiglia di utilizzare circuiti elettrici indipendenti per ogni alimentatore.
- Se possibile, installare un gruppo di continuità nelle propria sede.

Considerazioni sulla configurazione del rack

Quando si pianifica la configurazione del rack, è opportuno tenere presente alcuni punti:

- Se si installa uno chassis in un rack aperto, verificare che il telaio del rack non blocchi le porte di aspirazione o di sfiato.
- Assicurarsi che i rack chiusi godano di un'adeguata ventilazione. Assicurarsi che il rack non contenga un numero eccessivo di apparecchiature poiché tutti gli chassis generano calore. Un rack chiuso deve avere i pannelli laterali finestrati e una ventola per il raffreddamento.
- In un rack chiuso con una ventola nella parte superiore, il caldo generato dalle apparecchiature nella parte inferiore del rack può essere diretto verso l'alto e nelle porte di aspirazione delle apparecchiature sovrastanti presenti nel rack. Assicurarsi di fornire una ventilazione adeguata alle apparecchiature sul fondo del rack.
- L’uso di deflettori contribuisce a separare il flusso d'aria in uscita da quello in entrata e ad aspirare l'aria per il raffreddamento nello chassis. La collocazione ottimale dei deflettori dipende dal percorso del flusso d'aria all’interno del rack. Provando diverse soluzioni, si può determinare come posizionare i deflettori in modo efficace.

Installazione dell'hardware

In questa sezione viene descritta la procedura di installazione delle appliance nell'ambiente in uso. Include:

- **Montaggio dell'appliance**
- **Connessione dell'appliance alla rete**
- **Connessione all'appliance**
- **Configurazione della rete con la procedura di impostazione iniziale**

Montaggio dell'appliance

Le appliance Secure Network Analytics possono essere montate direttamente su un rack o un armadio da 19'' standard, su altro armadio disponibile o su una superficie piana. Per il montaggio dell'appliance in un rack o armadio, seguire le istruzioni incluse nei kit di montaggio guide. Quando si sceglie il luogo in cui installare l'appliance, assicurarsi che ci sia una distanza sufficiente dai pannelli anteriore e posteriore per consentire quanto segue:

- Sia possibile vedere chiaramente le spie del pannello anteriore
- L'accesso alle porte sul pannello posteriore sia sufficiente per un cablaggio senza alcuna restrizione
- La presa di alimentazione sul pannello posteriore sia raggiungibile da una sorgente di alimentazione CA condizionata.
- Il flusso d'aria intorno all'appliance e attraverso le feritoie non incontri ostruzioni.

Hardware incluso con l'appliance

I seguenti componenti hardware sono inclusi con le appliance Secure Network Analytics:

- Cavo di alimentazione CA
- Chiavi di accesso (per piastra anteriore)
- Kit di guide per il montaggio in rack o per il montaggio di piastrine per appliance più piccole
- Per Flow Collector 5210, cavo SFP da 10 GB

Hardware aggiuntivo richiesto

Sono richiesti i seguenti componenti hardware aggiuntivi:

- Viti di montaggio per rack da 19" standard
- UPS (Uninterruptible Power Supply, gruppo statico di continuità) per ciascuna appliance da installare
- Per la configurazione in locale (opzionale), procedere in uno dei seguenti modi:
    - Laptop con cavo video e cavo USB (per la tastiera)
    - Monitor con cavo video e tastiera con cavo USB

Connessione dell'appliance alla rete

Utilizzare la stessa procedura per connettere ogni appliance alla rete. L'unica differenza per la connessione consiste nel tipo di appliance di cui si dispone.

> ⚠ Non aggiornare il BIOS dell'appliance in quanto potrebbe causare problemi di funzionalità.

Per informazioni sulle specifiche di ciascuna appliance, fare riferimento alle schede tecniche di Secure Network Analytics.

> ℹ Tutti i componenti hardware di Cisco x2xx utilizzano la stessa piattaforma UCS, UCSC-C220-M5SX, eccetto Flow Collector 5210 DB, che utilizza UCSC-C240-M5SX. Gli elementi che variano nelle appliance sono le schede NIC, il processore, la memoria, i sistemi di archiviazione e RAID.

> ℹ Flow Collector 5210 è composto da due server connessi (motore e database) che funzionano come singola appliance. Per questo motivo, l'installazione è leggermente diversa dalle altre appliance. Innanzitutto, collegarle tra loro direttamente tramite un cavo Cross Connect SFP+ DA 10G. Quindi, connettersi alla rete.

Per collegare l'appliance alla rete:

1. Collegare un cavo Ethernet alla porta di gestione, nella parte posteriore dell'appliance.
2. Collegare almeno una porta monitor per i Flow Sensor e gli UDP Director.

   Per UDP Director HA, collegare due UDP Director tramite cavi crossover. Collegare la porta eth2 di un UDP Director alla porta eth2 del secondo UDP Director.

Analogamente, collegare la porta eth3 di ciascun UDP Director con un secondo cavo crossover. Il cavo può essere in fibra ottica o in rame.

Osservare l'etichetta Ethernet (eth2, eth3, ecc.) di ciascuna porta. Queste etichette corrispondono alle interfacce di rete (eth2, eth3, ecc.) visualizzate e possono essere configurate dalla Home page dell'interfaccia di amministrazione dell'appliance.

3. Collegare l'altra estremità dei cavi Ethernet allo switch di rete.
4. Collegare i cavi di alimentazione all'alimentatore. Alcune appliance dispongono di due alimentazioni: alimentatore 1 e alimentatore 2.

Connessione all'appliance

In questa sezione viene descritto come collegarsi all'appliance per poter modificare le password utente predefinite.

È possibile connettersi all'appliance in uno dei seguenti modi:

- con una tastiera e un monitor
- con un laptop (e un emulatore di terminale)

Nelle nuove appliance, SSH è disabilitato. Per abilitarlo, è necessario accedere all'interfaccia Web di amministrazione dell'appliance.

Connessione con una tastiera e un monitor

Per configurare l'indirizzo IP locale, procedere come segue:

1. Collegare il cavo di alimentazione all'appliance.
2. Premere il pulsante di accensione per attivare l'appliance. Attendere il completamento dell'avvio. Non interrompere il processo di avvio.

> Per fornire alimentazione, potrebbe essere necessario rimuovere il pannello anteriore.
>
> In alcuni modelli, le ventole dell'alimentatore si attivano con il sistema spento. Verificare che il LED sul pannello anteriore sia acceso.
>
> Collegare l'appliance a un UPS. In assenza di alimentazione, il sistema riporta un errore.

3. Collegare la tastiera:

- Se si dispone di una tastiera standard, collegarla al connettore della tastiera standard.
- Se si dispone di una tastiera USB, collegarla a un connettore USB.

4. Collegare il cavo video al connettore video. Viene visualizzato il prompt di accesso.
5. Proseguire alla sezione **Configurazione della rete con la procedura di impostazione iniziale**.

Connessione con un laptop

È anche possibile collegare l'appliance al laptop con un emulatore di terminale.

Per connettersi a un'appliance con un laptop:

1. Collegare il laptop all'appliance in uno dei seguenti modi:

- Collegare un cavo RS232 dal connettore della porta seriale (DB9) sul laptop alla porta console dell'appliance.
- Collegare un cavo crossover dalla porta Ethernet del laptop alla porta di gestione dell'appliance.

2. Collegare il cavo di alimentazione all'appliance.
3. Premere il pulsante di accensione per attivare l'appliance. Attendere il completamento dell'avvio. Non interrompere il processo di avvio.

> Per fornire alimentazione, potrebbe essere necessario rimuovere il pannello anteriore.
>
> In alcuni modelli, le ventole dell'alimentatore si attivano con il sistema spento. Verificare che il LED sul pannello anteriore sia acceso. Collegare l'appliance a un UPS. In assenza di alimentazione, il sistema riporta un errore.

4. Stabilire una connessione con l'appliance dal laptop.

   Utilizzare qualsiasi emulatore di terminale disponibile per comunicare con l'appliance.

5. Applicare le seguenti impostazioni:

- BPS: 115200
- Bit di dati: 8
- Bit di stop: 1
- Parità: Nessuna
- Controllo del flusso: Nessuno

  Vengono visualizzati la schermata e il prompt di accesso.

6. Proseguire alla prossima sezione, **Configurazione della rete con la procedura di impostazione iniziale**.

Configurazione della rete con la procedura di impostazione iniziale

Dopo aver effettuato il collegamento all'appliance, seguire la procedura di impostazione iniziale per configurare i parametri della rete, inclusi gli indirizzi IP. Tenere presente quanto segue:

- Se si implementa un Manager 2210 o un Flow Collector 4210 con un Data Store, oltre a configurare gli indirizzi IP è anche possibile configurare il Manager o il Flow Collector per consentirne l'uso con un Data Store e il tipo di porta fisica per la gestione dell'interfaccia `eth0`.

  > ⚠ Dopo aver scelto di configurare il Manager o il Flow Collector in modo da consentirne l'uso con un Data Store, non è possibile aggiornare la configurazione dell'appliance per modificare questa opzione. Se si sceglie l'opzione sbagliata, sarà necessario effettuare il reset dell'appliance alle impostazioni di fabbrica. Abilitare questa opzione solo se si intende implementare un Data Store nella rete.

- Se l'appliance è un Data Node, è possibile configurare il tipo di porta fisica da utilizzare come porta di gestione `eth0`, l'indirizzo IP e relative informazioni per `eth2` o il port-channel `eth2`/`eth3` per le comunicazioni con il Data Node.

Per ulteriori informazioni sull'installazione delle appliance Manager 2210, FC 4210 e Data Node, vedere la guida all'installazione e alla configurazione hardware di Secure Network Analytics Data Store.

Dopo aver configurato gli indirizzi IP e le porte, cambiare le password utente.

> La prima volta che si accede alla configurazione del sistema, viene avviata l'impostazione guidata iniziale che guida l'utente nella configurazione iniziale dell'appliance. Se si esce dall'impostazione iniziale prima di aver completato la procedura guidata, al successivo accesso alla configurazione di sistema, la procedura di impostazione guidata iniziale viene avviata nuovamente.

A seconda dell'appliance, passare alla sezione seguente:

- **Appliance compatibili con il Data Store (Manager 2210, FC 4210)**
- **Configurazione generale delle appliance Secure Network Analytics**
- **Configurazione del Data Node**

Configurazione generale delle appliance Secure Network Analytics

Su tutte le appliance eccetto i Data Node, il Manager 2210 e l'FC 4210, nell'impostazione iniziale viene visualizzato quanto segue:

- Configurazione dell'indirizzo IP e delle informazioni di gestione dell'appliance

Configurazione dell'indirizzo IP e delle informazioni di gestione dell'appliance

L'indirizzo IP di gestione eth0 e le relative informazioni vengono specificate nell'impostazione iniziale. Sulla maggior parte delle appliance, si tratta della prima configurazione nell'impostazione iniziale.

Operazioni preliminari

- Se si sta configurando un Data Node, andare a Configurazione dei Data Node.
- Se si sta configurando un Manager o un Flow Collector compatibile con il Data Store, andare a Appliance compatibili con il Data Store (Manager 2210, FC 4210).
- Se si sta configurando un'altra appliance Secure Network Analytics, iniziare dal passaggio 1.

Procedura

1. Accedere al programma di configurazione del sistema:
    - Se si sta configurando un Data Node o un'appliance compatibile con il Data Store, digitare `root` e premere **Invio**. Se si sta configurando un'altra appliance, digitare `sysadmin` e premere **Invio**.

> **i** Le autorizzazioni `root` sono richieste per configurare correttamente il Data Store e la sua compatibilità.

- Quando viene visualizzato il prompt della password, digitare **lan1cope**, quindi premere **Invio**.
- Al prompt successivo, digitare **SystemConfig**, quindi premere **Invio**.

2. Al primo accesso alla configurazione di sistema sull'appliance viene visualizzata la procedura di impostazione iniziale.

   A tutti gli accessi successivi viene aperto il menu della configurazione di sistema. Selezionare **Management** (Gestione), quindi premere **Invio**.
3. In **IP address**, immettere l'indirizzo IP dell'appliance.
4. In **Netmask**, immettere una netmask per la rete.
5. In **Gateway**, immettere l'indirizzo gateway per l'indirizzo IP dell'appliance.
6. In **Broadcast**, immettere un indirizzo di trasmissione per l'appliance.
7. In **Hostname**, immettere un nome host per l'appliance.
8. In **Domain**, immettere un dominio per l'appliance.
9. Selezionare **Select** (Seleziona), quindi **Yes** (Sì) per confermare le informazioni immesse.

   Questa è l'ultima opzione di configurazione nell'impostazione iniziale. L'appliance viene riavviata per applicare le modifiche. Al termine, viene visualizzata la pagina di accesso.

Come procedere

- Cambiare le password utente. Per ulteriori informazioni, vedere **Modifica della password utente sysadmin**.

Appliance compatibili con il Data Store (Manager 2210, FC 4210)

Su Manager 2210 e FC 4210, nell'impostazione iniziale viene visualizzata la seguente configurazione:

1. Configurazione della porta di gestione fisica eth0
2. Configurazione dell'indirizzo IP e delle informazioni di gestione dell'appliance
3. Configurazione della compatibilità di Data Store
4. Configurare l'uso di Security Analytics e Logging On Prem

Configurazione della porta di gestione fisica eth0

Se si configura un Manager o un Flow Collector compatibile con il Data Store e si sta implementando un Data Store, è possibile configurare facoltativamente `eth0` come porta SFP+ DAC al posto della porta in rame BASE-T predefinita. Su queste appliance, si tratta della prima configurazione nell'impostazione iniziale.

Operazioni preliminari

- Se si sta configurando un Data Node, un Manager compatibile con un Data Store o un Flow Collector, vedere la scheda tecnica di Secure Network Analytics per l'appliance in uso per informazioni sulle porte SFP+ e BASE-T supportate.
- Se si sta configurando un Data Node, andare a Configurazione dei Data Node.
- Se si sta configurando un'appliance Secure Network Analytics diversa dalle appliance compatibili con il Data Store, vedere Configurazione generale delle appliance Secure Network Analytics.

Procedura

1. Accedere al programma di configurazione del sistema:
   - Immettere **root**, quindi premere **Invio**.

     > Per configurare correttamente la compatibilità del Data Store sono richieste autorizzazioni `root`.

   - Quando viene visualizzato il prompt della password, digitare **lan1cope**, quindi premere **Invio**.
   - Al prompt successivo, digitare **SystemConfig**, quindi premere **Invio**.
2. Al primo accesso alla configurazione di sistema sull'appliance viene visualizzata la procedura di impostazione iniziale e la configurazione dell'ordine delle porte. Andare al passaggio 5.

   A tutti gli accessi successivi viene aperto il menu della configurazione di sistema. Selezionare **Management** (Gestione), quindi premere **Invio**.
3. Dal menu System Configuration (Configurazione di sistema), selezionare **Network** (Rete), quindi premere **Invio**.
4. Selezionare **Port Order** (Ordine delle porte), quindi premere Invio.
5. Sono disponibili le seguenti opzioni:
   - Selezionare **LOM** per consentire all'appliance di utilizzare una porta in rame BASE-T per eth0.

- Selezionare **SFP+** per consentire all'appliance di utilizzare una porta in fibra SFP+ per eth0.

6. Selezionare **OK** per confermare la selezione.

Come procedere

- Configurare l'indirizzo IP e le informazioni di gestione della porta eth0. Vedere la procedura successiva.

Configurazione dell'indirizzo IP e delle informazioni di gestione dell'appliance

L'indirizzo IP di gestione eth0 e le relative informazioni vengono specificate nell'impostazione iniziale. Sulle appliance compatibili con il Data Store, questa configurazione viene eseguita dopo la configurazione della porta di gestione fisica eth0.

Operazioni preliminari

- Se si sta configurando un Manager o un Flow Collector compatibile con il Data Store, dopo aver configurato l'ordine delle porte, nell'impostazione guidata iniziale viene visualizzata la configurazione della gestione di `eth0`. Andare al passaggio 3.

Procedura

1. Accedere al programma di configurazione del sistema:
   - Se si sta configurando un'appliance compatibile con il Data Store, digitare `root` e premere **Invio**.

     > Le autorizzazioni `root` sono richieste per configurare correttamente il Data Store e la sua compatibilità.

   - Quando viene visualizzato il prompt della password, digitare **lan1cope**, quindi premere **Invio**.
   - Al prompt successivo, digitare **SystemConfig**, quindi premere **Invio**.
2. Al primo accesso alla configurazione di sistema sull'appliance viene visualizzata la procedura di impostazione iniziale.

   A tutti gli accessi successivi viene aperto il menu della configurazione di sistema. Selezionare **Management** (Gestione), quindi premere **Invio**.
3. In **IP address**, immettere l'indirizzo IP dell'appliance.
4. In **Netmask**, immettere una netmask per la rete.
5. In **Gateway**, immettere l'indirizzo gateway per l'indirizzo IP dell'appliance.

6. In **Broadcast**, immettere un indirizzo di trasmissione per l'appliance.
7. In **Hostname**, immettere un nome host per l'appliance.
8. In **Domain**, immettere un dominio per l'appliance.
9. Selezionare **Select** (Seleziona), quindi **Yes** (Sì) per confermare le informazioni immesse.

Come procedere

- Configurare l'appliance per l'utilizzo senza un Data Store. Per ulteriori informazioni, vedere la procedura seguente.

Configurazione dell'utilizzo di Data Store

Configurare il Manager 2210 o l'FC 4210 in modo che possano essere utilizzati con un Data Store. I Flow Connector si connetteranno al Data Store e il Manager interrogherà il Data Store.

> ⚠ Dopo aver scelto di configurare il Manager o il Flow Collector in modo da consentirne l'uso con un Data Store, non è possibile aggiornare la configurazione dell'appliance per modificare questa opzione. Se si sceglie l'opzione sbagliata, sarà necessario effettuare il reset dell'appliance alle impostazioni di fabbrica. Abilitare questa opzione **solo se** si intende implementare un Data Store nella rete.

> ℹ Se si implementa un Data Store, i Manager e i Flow Collector devono essere configurati in modo da poter essere utilizzati con un Data Store. Non è possibile configurare i Flow Collector in modo che alcuni si connettano al Data Store e altri si connettano direttamente al Manager.

Operazioni preliminari

- Nell'impostazione iniziale, la configurazione di sistema visualizza la configurazione del Data Store una volta specificato l'indirizzo IP dell'appliance. Andare al passaggio 3.

Procedura

1. Dal menu System Configuration (Configurazione di sistema), selezionare **Advanced** (Avanzate) e premere **Invio**.
2. Selezionare **Data Store**, quindi premere Invio.

3. Selezionare **Yes** (Sì) per configurare la compatibilità dell'appliance con un Data Store.

> ⚠ Dopo aver scelto di configurare il Manager o il Flow Collector in modo da consentirne l'uso con un Data Store, non è possibile aggiornare la configurazione dell'appliance per modificare questa opzione. Se si sceglie l'opzione sbagliata, sarà necessario effettuare il reset dell'appliance alle impostazioni di fabbrica. Abilitare questa opzione **solo se** si intende implementare un Data Store nella rete.

4. Selezionare **OK** per confermare la selezione.

Come procedere

- Configurare Security Analytics and Logging On Prem. Per ulteriori informazioni, vedere la procedura seguente.

Configurazione di Security Analytics and Logging On Prem

Configurare il Manager 2210 o il FC 4210 per Security Analytics and Logging On Prem, in modo da utilizzare l'implementazione di Secure Network Analytics per memorizzare le informazioni sugli eventi di Firepower. Il Flow Collector acquisirà le informazioni sugli eventi di Firepower e le invierà al Data Store per l'archiviazione. A questo punto è possibile richiedere informazioni sull'evento di Firepower dal Manager o dal Firepower Management Center.

Se si configura Security Analytics and Logging On Prem, è anche necessario installare l'app Security Analytics and Logging On Prem su Manager. Vedere Dati analitici sulla sicurezza e registrazione: guida all'integrazione di eventi Firepower per ulteriori informazioni.

> ⚠ Dopo aver scelto di configurare il Manager o il Flow Collector in modo da consentirne l'uso con Security Analytics and Logging On Prem, non è possibile aggiornare la configurazione dell'appliance per modificare questa opzione. Se si sceglie l'opzione sbagliata, sarà necessario effettuare il reset dell'appliance alle impostazioni di fabbrica. Abilitare questa opzione **solo se** si prevede di utilizzare Secure Network Analytics per Security Analytics and Logging On Prem in modo da archiviare le informazioni sugli eventi di Firepower.

Operazioni preliminari

- Nell'impostazione iniziale, la configurazione di sistema visualizza la configurazione di Security Analytics and Logging On Prem una volta finito di configurare l'utilizzo del Data Store.

Procedura

1. Selezionare **Yes** per attivare Security Analytics and Logging On Prem e inserire le informazioni sugli eventi del firewall dall'implementazione Firepower. Attenzione: questa operazione disabilita la raccolta NetFlow sul Flow Collector.

   > ⚠ Dopo aver scelto di configurare il Manager o il Flow Collector in modo da consentirne l'uso con Security Analytics and Logging On Prem, non è possibile aggiornare la configurazione dell'appliance per modificare questa opzione. Se si sceglie l'opzione sbagliata, sarà necessario effettuare il reset dell'appliance alle impostazioni di fabbrica. Abilitare questa opzione **solo se** si prevede di utilizzare Secure Network Analytics per Security Analytics and Logging On Prem in modo da archiviare le informazioni sugli eventi di Firepower.

2. Selezionare **No** per disabilitare Security Analytics and Logging On Prem. È possibile importare NetFlow sul Flow Collector. Non è possibile inserire le informazioni sugli eventi del firewall dalla propria implementazione di Firepower.
3. Selezionare **OK** per confermare la selezione.

   Questa è l'ultima opzione di configurazione nell'impostazione iniziale. L'appliance viene riavviata per applicare le modifiche. Al termine, viene visualizzata la pagina di accesso.

Configurazione del Data Node

Sui Data Node, nell'impostazione iniziale viene visualizzata la seguente configurazione:

1. Configurazione della porta di gestione fisica eth0
2. Configurazione dell'indirizzo IP e delle informazioni di gestione dell'appliance
3. Configurazione delle porte eth2 ed eth3 per le comunicazioni tra Data Node

Configurazione della porta di gestione fisica eth0

Se si configura un Data Node, è possibile facoltativamente specificare `eth0` come porta in rame BASE-T al posto della porta SFP+ DAC predefinita. Su queste appliance, si tratta della prima configurazione nell'impostazione iniziale.

Operazioni preliminari

- Se si sta configurando un Data Node, vedere la scheda delle specifiche di Secure Network Analytics per l'appliance in uso per informazioni sulle porte SFP+ e BASE-T supportate.

- Se si sta configurando un Manager o un Flow Collector compatibile con il Data Store, andare a Appliance compatibili con il Data Store (Manager 2210, FC 4210).
- Se si sta configurando un'appliance Secure Network Analytics diversa dalle appliance compatibili con il Data Store, vedere Configurazione generale delle appliance Secure Network Analytics.

Procedura

1. Accedere al programma di configurazione del sistema:
   - Immettere **root**, quindi premere **Invio**.

     > Per configurare correttamente la compatibilità del Data Store sono richieste autorizzazioni `root`.

   - Quando viene visualizzato il prompt della password, digitare **lan1cope**, quindi premere **Invio**.
   - Al prompt successivo, digitare **SystemConfig**, quindi premere **Invio**.
2. Al primo accesso alla configurazione di sistema sull'appliance viene visualizzata la procedura di impostazione iniziale e la configurazione dell'ordine delle porte. Andare al passaggio 5.

   A tutti gli accessi successivi viene aperto il menu della configurazione di sistema. Selezionare **Management** (Gestione), quindi premere **Invio**.
3. Dal menu System Configuration (Configurazione di sistema), selezionare **Network** (Rete), quindi premere **Invio**.
4. Selezionare **Port Order** (Ordine delle porte), quindi premere Invio.
5. Sono disponibili le seguenti opzioni:
   - Selezionare **SFP+** per consentire all'appliance di utilizzare una porta in fibra SFP+ per eth0.
   - Selezionare **LOM** per consentire all'appliance di utilizzare una porta in rame BASE-T per eth0.
6. Selezionare **OK** per confermare la selezione.

Come procedere

- Configurare l'indirizzo IP e le informazioni di gestione della porta eth0. Vedere la procedura successiva.

Configurazione dell'indirizzo IP e delle informazioni di gestione dell'appliance

L'indirizzo IP di gestione eth0 e le relative informazioni vengono specificate nell'impostazione iniziale.

Operazioni preliminari

- Se si sta configurando un Data Node, dopo aver configurato l'ordine delle porte, nell'impostazione iniziale guidata viene visualizzata la configurazione della gestione di `eth0`. Andare al passaggio 3.

Procedura

1. Accedere al programma di configurazione del sistema:
   - Se si sta configurando un Data Node, digitare `root` e premere **Invio**.

     > Le autorizzazioni `root` sono richieste per configurare correttamente il Data Store e la sua compatibilità.

   - Quando viene visualizzato il prompt della password, digitare **lan1cope**, quindi premere **Invio**.
   - Al prompt successivo, digitare **SystemConfig**, quindi premere **Invio**.
2. Al primo accesso alla configurazione di sistema sull'appliance viene visualizzata la procedura di impostazione iniziale.

   A tutti gli accessi successivi viene aperto il menu della configurazione di sistema. Selezionare **Management** (Gestione), quindi premere **Invio**.
3. In **IP address**, immettere l'indirizzo IP dell'appliance.
4. In **Netmask**, immettere una netmask per la rete.
5. In **Gateway**, immettere l'indirizzo gateway per l'indirizzo IP dell'appliance.
6. In **Broadcast**, immettere un indirizzo di trasmissione per l'appliance.
7. In **Hostname**, immettere un nome host per l'appliance.
8. In **Domain**, immettere un dominio per l'appliance.
9. Selezionare **Select** (Seleziona), quindi **Yes** (Sì) per confermare le informazioni immesse.

Come procedere

- Configurare le informazioni sulla gestione delle porte di comunicazione nel Data Node. Per ulteriori informazioni, vedere **Configurazione delle porte eth2 ed eth3 per le comunicazioni tra Data Node**.

Configurazione delle porte eth2 ed eth3 per le comunicazioni tra Data Node

Quando si configura un'appliance Data Node, configurare la porta per le comunicazioni tra Data Node con un indirizzo IP non instradabile. È possibile configurare uno dei seguenti elementi:

- `eth2`
- port-channel contenente `eth2` ed `eth3`

> È necessario assegnare indirizzi IP non indirizzabili dal blocco CIDR `169.254.42.0/24`.

Operazioni preliminari

- Per informazioni sulle porte SFP+ `eth2` e `eth3`, vedere la scheda tecnica di Secure Network Analytics per l'appliance in uso. Notare che `eth2` e `eth3` dipendono dalla configurazione di `eth0`.
- Nell'impostazione iniziale, in System Configuration (Configurazione di sistema) viene visualizzata la configurazione di `eth2` o del port-channel `eth2/eth3` dopo aver completato la configurazione delle informazioni di gestione `eth0` dell'appliance. Andare al passaggio 3.

Procedura

1. Dal menu System Configuration (Configurazione di sistema), selezionare **Network** (Rete), quindi premere **Invio**.
2. Selezionare **Node Communications** (Comunicazioni nodi), quindi premere Invio.
3. Selezionare la configurazione della porta di comunicazione tra Data Node. Sono disponibili le seguenti opzioni:
    - Selezionare **Yes** (Sì) per aggregare `eth2` ed `eth3` come port-channel per le comunicazioni tra Data Node.
    - Selezionare **No** per utilizzare `eth2` per le comunicazioni tra Data Node.
4. Immettere un **indirizzo IP** non indirizzabile dal blocco CIDR `169.254.42.0/24` per `eth2` o il port-channel `eth2/eth3`.

5. In **Netmask**, immettere la netmask `255.255.255.0` per questo indirizzo IP.
6. In **Gateway**, immettere un indirizzo gateway per questo indirizzo IP.
7. In **Broadcast**, immettere un indirizzo di trasmissione per questo indirizzo IP.
8. Selezionare **Select** (Seleziona), quindi **Yes** (Sì) per confermare le informazioni immesse.

   Questa è l'ultima opzione di configurazione nell'impostazione iniziale. L'appliance viene riavviata per applicare le modifiche. Al termine, viene visualizzata la pagina di accesso.

Come procedere

- Cambiare le password utente. Per ulteriori informazioni, vedere **Modifica della password utente sysadmin**.

Modifica della password utente sysadmin

Per garantire la sicurezza della rete, cambiare la password sysadmin predefinita delle appliance.

Modifica della password sysadmin

Operazioni preliminari

- Accedere alla console dell'appliance come **sysadmin**.
- Accedere alla configurazione di sistema.

Procedura

1. Nel menu di configurazione del sistema, selezionare **Password** e premere **Invio**.

   Se l'elenco predefinito degli host attendibili è stato modificato, verificare che ciascuna appliance Secure Network Analytics sia presente nell'elenco degli host attendibili di tutte le altre appliance Secure Network Analytics implementate. In caso contrario, le appliance non potranno comunicare tra di loro.

   Sotto il menu viene visualizzato un prompt per la password corrente.
2. Digitare la password corrente e premere **Invio**.

   Viene visualizzato il prompt per una nuova password.
3. Digitare la nuova password e premere **Invio**.

   La password deve contenere da 8 a 30 caratteri alfanumerici senza spazi. È inoltre possibile utilizzare i seguenti caratteri speciali: `$.~!@#%_=?:,{}()`
4. Digitare nuovamente la password e premere **Invio**.

5. Una volta accettata la password, premere **Invio** di nuovo per tornare al menu di configurazione del sistema.
6. Continuare alla sezione **Modifica della password utente root**.

Modifica della password utente root

Dopo aver modificato la password utente sysadmin predefinita, modificare quella dell'utente root per garantire una maggiore protezione della rete.

Modifica della password utente root

Operazioni preliminari

- Accedere alla console dell'appliance come **sysadmin**.
- Accedere alla configurazione di sistema.

Procedura

1. Andare alla shell root.
2. Nel menu di configurazione del sistema, selezionare **Advanced** (Avanzate) e premere **Invio**. Viene visualizzato il menu Advanced (Avanzate).
3. Selezionare **RootShell**, quindi premere **Invio**.

   Viene visualizzato il prompt per la password root.
4. Digitare la password root corrente e premere **Invio**. Viene visualizzato il prompt per la shell root.
5. Digitare **SystemConfig**, quindi premere **Invio**.

   In questo modo, si torna al menu di configurazione del sistema da dove è possibile modificare la password root.
6. Selezionare **Password**, quindi premere **Invio**. Sotto il menu viene visualizzato il prompt per la password.
7. Digitare la nuova password root e premere **Invio**. Viene visualizzato un secondo prompt.
8. Digitare nuovamente la password root, quindi premere **Invio**.
9. Dopo aver modificato la password, premere **Invio**. A questo punto, entrambe le password sysadmin e root predefinite sono state modificate. In questo modo, si torna al menu della console di configurazione del sistema.
10. Selezionare **Cancel** (Annulla) e premere **Invio**. La console di configurazione del sistema si chiude e viene visualizzato il prompt della shell root.

11. Digitare **exit** e premere **Invio**. Viene visualizzato il prompt di accesso.
12. Premere **Ctrl+Alt** per uscire dall'ambiente della console.

A questo punto è possibile configurare l'appliance. Per configurare l'appliance, consultare la guida alla configurazione di **Secure Network Analytics System** per la versione software in uso. La serie x2xx è compatibile con le versioni software Secure Network Analytics 7.x.

Configurazione dell'appliance

A questo punto è possibile configurare l'appliance. Per configurare l'appliance, consultare la guida alla configurazione di **Secure Network Analytics System** e la guida all'implementazione e alla configurazione hardware di Secure Network Analytics Data Store per la versione software installata. La serie x2xx è compatibile con le versioni software Secure Network Analytics 7.x.

Contattare il supporto

Per richiedere assistenza tecnica procedere come segue:

- Contattare il partner Cisco locale
- Contattare il supporto Cisco
- Per aprire una richiesta di assistenza via Web: http://www.cisco.com/c/en/us/support/index.html
- Per aprire una richiesta di assistenza tramite e-mail: tac@cisco.com
- Per contattare il supporto telefonico chiamare il numero: 1-800-553-2447 (USA)
- Per conoscere i numeri dell'assistenza in tutto il mondo: https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

Informazioni sul copyright