Cisco Stealthwatch

Serie x210 Guida all'installazione dell'hardware

Table of Contents

Introduzione

Panoramica

In questa guida viene illustrato come installare le appliance hardware Stealthwatch serie x210. Vengono descritti i componenti Stealthwatch 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 Stealthwatch. Componenti hardware della serie x210:

Appliance	Codice prodotto
Stealthwatch Flow Collector 4210	ST-FC4210-K9
Stealthwatch Flow Collector 5210 Database	ST-FC5210-E
Stealthwatch Flow Collector 5210 Database	ST-FC5210-D
Stealthwatch Flow Sensor 1210	ST-FS1210-K9
Stealthwatch Flow Sensor 3210	ST-FS3210-K9
Stealthwatch Flow Sensor 4210	ST-FS4210-K9
Stealthwatch Management Console 2210	ST-SMC2210-K9
Stealthwatch UDP Director 2210	ST-UDP2210-K9

Destinatari

La presente guida è rivolta agli addetti all'installazione dei componenti hardware Stealthwatch. Si suppone che i destinatari della presente guida abbiano nozioni generali sull'installazione delle apparecchiature di rete (Flow Sensor, Flow Collector, UDP Director e Stealthwatch Management Console).

> Per informazioni sulla configurazione delle appliance Stealthwatch, consultare la **guida di installazione e configurazione Stealthwatch** adeguata alla versione di software interessata. La serie x210 è compatibile con le versioni software Stealthwatch 7.x.

Come usare la guida

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

Capitolo	Descrizione
2 - **Considerazioni sulla pre-configurazione**	Componenti Stealthwatch, posizionamento e configurazione del firewall per le comunicazioni
3 - **Preparazione dell'installazione**	Linee guida, raccomandazioni e avvertenze per la sicurezza
4 - **Installazione**	Montaggio e installazione dei componenti hardware di Stealthwatch

Abbreviazioni comuni

Nella guida sono presenti 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

Abbreviazione	Descrizione
UPS	Uninterruptible Power Supply, gruppo statico di continuità
VLAN	Virtual Local Area Network, LAN virtuale

Preparazione dell'installazione

Avvertenze relative all'installazione

Leggere il documento delle informazioni sulla conformità alle normative e sulla sicurezza prima di installare le appliance Stealthwatch serie x210.

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. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device.

CONSERVARE QUESTE ISTRUZIONI

Avvertenza 1005: interruttore

Questo prodotto dipende dall'impianto dell'edificio per quanto riguarda la protezione contro cortocircuiti (sovracorrente). Assicurarsi che il dispositivo di protezione non abbia una classe superiore a 120, 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, installare 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 contro 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

Questo prodotto dipende dall'impianto dell'edificio per quanto riguarda la protezione contro cortocircuiti (sovracorrente). Assicurarsi che il dispositivo di protezione non abbia una classe superiore a 120, 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, utilizzare 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 pat-tern 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.

Mantenere la sicurezza rispetto all'elettricità

> ⚠ 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.

Considerazioni sulla pre-configurazione

In questa sezione vengono esaminate le considerazioni da fare prima di installare e configurare le appliance Stealthwatch. Viene descritto dove posizionare le appliance Stealthwatch e come integrarle nella propria rete. Include:

- **Accesso con la Password predefinita CIMC**
- **Informazioni sulle appliance Stealthwatch**
- **Posizionamento delle appliance**
- **Porte di comunicazione**
- **Integrazione del Flow Sensor nella propria 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 dello stato hardware. Utilizzare la seguente password predefinita per accedere al CIMC:

`password`.

Una volta effettuato l'accesso, modificare la password predefinita per garantire una maggiore protezione della propria rete.

Informazioni sulle appliance Stealthwatch

Stealthwatch comprende diverse appliance hardware che raccolgono, analizzano e presentano le informazioni relative alla rete per migliorare le prestazioni e la sicurezza della stessa. In questa sezione vengono descritte le appliance Stealthwatch serie x210.

> Per ulteriori informazioni, fare riferimento alle schede tecniche di ciascuna appliance Stealthwatch serie x210.

Stealthwatch Management Console 2210

Stealthwatch Management Console gestisce, coordina, configura e organizza tutti i diversi componenti del sistema. Il software Stealthwatch consente di accedere all'UI 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 relativamente ai segmenti critici dell'azienda. Grazie all'indipendenza della piattaforma basata su Java, Stealthwatch Management Console consente quanto segue:

- Gestione centralizzata, configurazione e reporting per un numero massimo di 25 Stealthwatch 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

Stealthwatch Flow Collector 4210 e 5210

Stealthwatch Flow Collector raccoglie i dati NetFlow, cFlow, J-Flow, Packeteer 2, NetStream e IPFIX per fornire la sicurezza di rete basata sui 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.

> 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 Stealthwatch ha identificato il comportamento, il sistema può intraprendere l'azione configurata, se disponibile, per quel tipo di comportamento.

Stealthwatch Flow Sensor 1210, 3210 e 4210

Stealthwatch 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 test access port (TAP) 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 il Flow Collector NetFlow v9, è possibile ottenere statistiche dettagliate sul traffico da NetFlow. In combinazione con Stealthwatch Flow Collector, il Flow Sensor offre informazioni più dettagliate 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 del pacchetto, può calcolare il tempo di round-trip (RTT), il tempo di risposta del server (SRT) e la perdita di pacchetti per le sessioni TCP. Sono inclusi tutti quei campi nei record NetFlow che vengono inviati al Flow Collector.

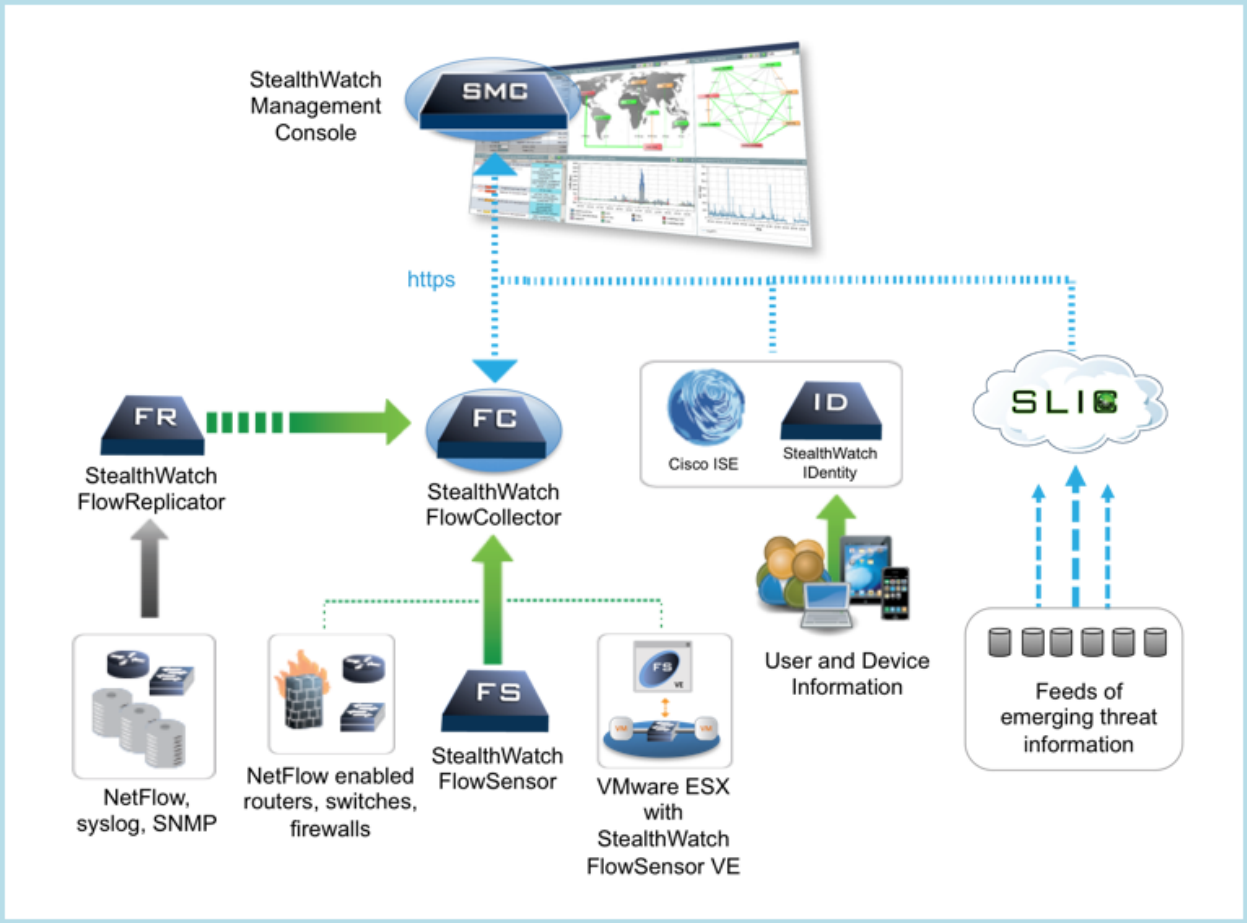
Stealthwatch UDP Director 2210

Stealthwatch 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 sotto, è possibile implementare le appliance Stealthwatch in modo strategico per fornire una copertura ottimale dei segmenti di rete principale attraverso la rete, sia nella rete interna, che nella zona perimetrale che nella DMZ.



Posizionamento della Stealthwatch Management Console

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

Se si dispone di una coppia failover di Stealthwatch Management Console, si consiglia di installare le console primaria e secondaria in punti distinti e separati. Questa strategia consentirà un ripristino di emergenza più facile in caso di necessità.

Posizionamento di Stealthwatch Flow Collector

In quanto dispositivo di raccolta e monitoraggio, Stealthwatch Flow Collector deve essere installato in un punto della rete accessibile ai dispositivi NetFlow o sFlow che devono inviare dati a un Flow Collector e a tutti i dispositivi che dovranno essere utilizzati per accedere all'interfaccia di gestione.

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 di Stealthwatch Flow Sensor

In quanto dispositivo di monitoraggio passivo, Stealthwatch 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 scoprire 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 Stealthwatch UDP Director

L'unico requisito del posizionamento di Stealthwatch UDP Director è che disponga di un percorso di comunicazione senza ostruzioni con il resto delle appliance Stealthwatch.

Configurazione del firewall per le comunicazioni

Affinché le appliance comunichino correttamente, è necessario configurare la rete in modo che i firewall o gli elenchi di controllo degli accessi non blocchino le connessioni richieste. Utilizzare lo schema e le tabelle mostrate in questa sezione per configurare la rete in modo che le appliance possano comunicare attraverso la rete.

Rivolgersi all'amministratore di rete per assicurarsi che le seguenti porte siano aperte e non abbiano accesso limitato:

- TCP 22
- TCP 25
- TCP 389
- TCP 443
- TCP 2393
- TCP 5222

- UDP 53
- UDP 123
- UDP 161
- UDP 162
- UDP 389
- UDP 514
- UDP 2055
- UDP 6343

Porte di comunicazione

Nella tabella seguente viene mostrato l'uso delle porte in Stealthwatch:

Da (Client)	A (Server)	Porta	Protocollo
PC utente amministratore	Tutti i dispositivi	TCP/443	HTTPS
Tutti i dispositivi	Origine ora rete	UDP/123	NTP
Active Directory	Stealthwatch Management Console	TCP/389, UDP/389	LDAP
AnyConnect	Endpoint Concentratore	UDP/2055	NetFlow
Cisco ISE	Stealthwatch Management Console	TCP/443	HTTPS
Cisco ISE	Stealthwatch Management Console	TCP/5222	XMPP
Concentratore endpoint	Flow Collector	UDP/2055	NetFlow
Origini log esterni	Stealthwatch Management Console	UDP/514	SYSLOG
Flow Collector	Stealthwatch Management Console	TCP/443	HTTPS
SLIC	Stealthwatch Management Console	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

Da (Client)	A (Server)	Porta	Protocollo
Flow Sensor	Stealthwatch Management Console	TCP/443	HTTPS
Flow Sensor	Flow Collector - NetFlow	UDP/2055	NetFlow
Identità	Stealthwatch Management Console	TCP/2393	SSL
Esportatori NetFlow	Flow Collector - NetFlow	UDP/2055*	NetFlow
Esportatori sFlow	Flow Collector - sFlow	UDP/6343*	sFlow
Stealthwatch Management Console	Cisco ISE	TCP/443	HTTPS
Stealthwatch Management Console	DNS	UDP/53	DNS
Stealthwatch Management Console	Flow Collector	TCP/443	HTTPS
Stealthwatch Management Console	Flow Sensor	TCP/443	HTTPS
Stealthwatch Management Console	Identità	TCP/2393	SSL
Stealthwatch Management Console	Esportatori di flussi	UDP/161	SNMP
Stealthwatch Management Console	Concentratore endpoint	UDP.2055	HTTPS
PC utente	Stealthwatch Management Console	TCP/443	HTTPS

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

La seguente tabella è valida per le configurazioni opzionali determinate dalle esigenze di rete:

Da (Client)	A (Server)	Porta	Protocollo
Tutti i dispositivi	PC utente	TCP/22	SSH
Stealthwatch Management Console	Gestione eventi di terze parti	UDP/162	Trap SNMP
Stealthwatch Management Console	Gestione eventi di terze parti	UDP/514	SYSLOG
Stealthwatch Management Console	Gateway e-mail	TCP/25	SMTP
Stealthwatch Management Console	SLIC	TCP/443	SSL
PC utente	Tutti i dispositivi	TCP/22	SSH

Nel seguente schema vengono mostrate le varie connessioni utilizzate da Stealthwatch. Le porte contrassegnate come facoltative sono quelle che possono essere utilizzate in base alle proprie esigenze di rete.

Integrazione del Flow Sensor nella propria rete

Stealthwatch 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 Stealthwatch Flow Sensor nella propria 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 ripeterà la direzione della trasmissione su porte separate. Pertanto, l'uso di una TAP è il modo più affidabile di utilizzare il Flow Sensor. Il tipo di TAP da utilizzare dipende dalla propria rete.

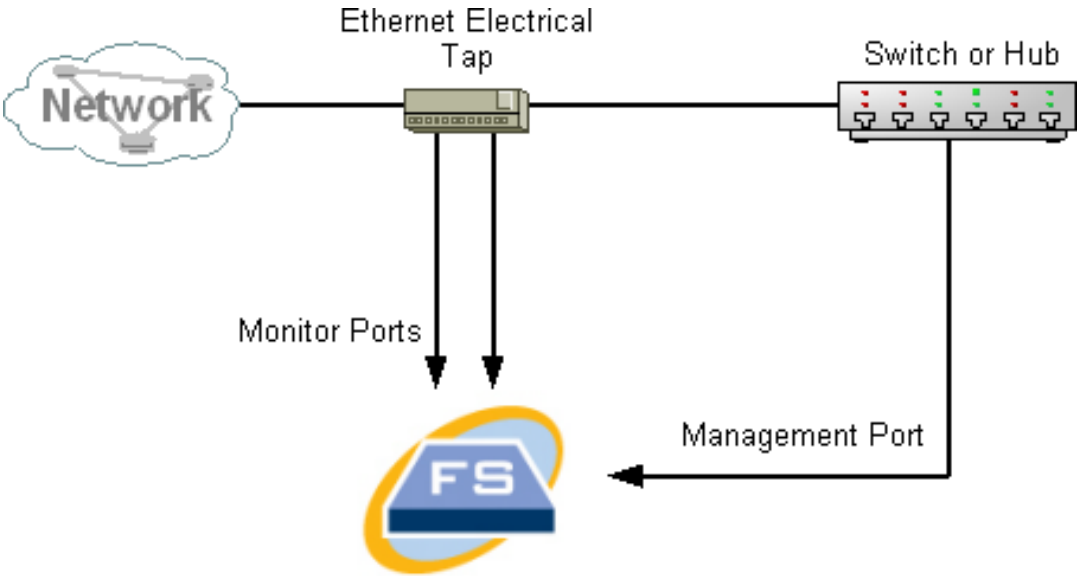
In questa sezione vengono descritti i metodi di utilizzo delle TAP:

- **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

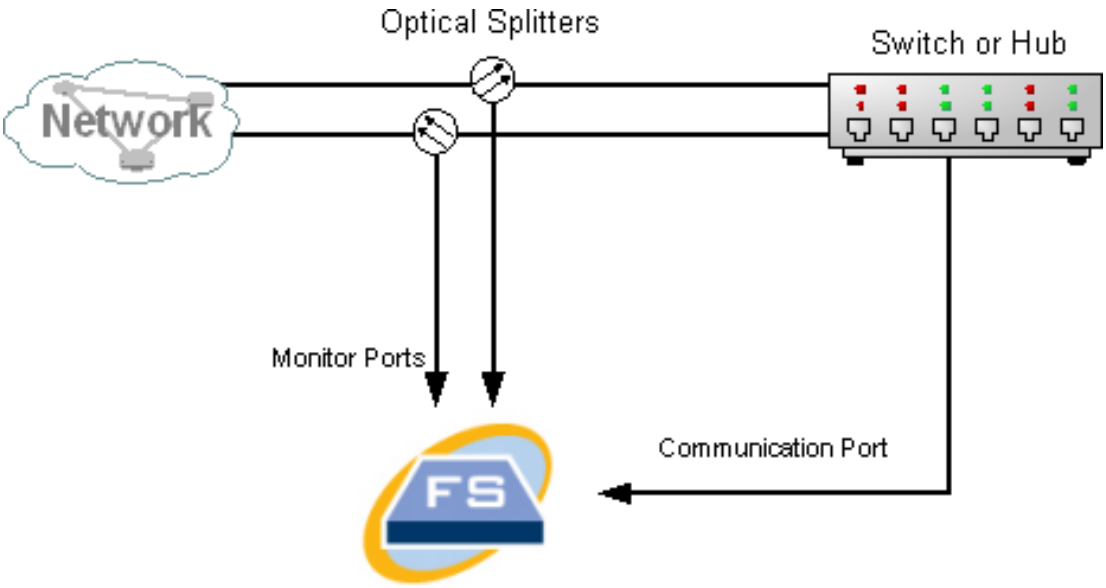
Nell'esempio seguente, il Flow Sensor è connesso a una TAP Ethernet elettrica. Per effettuare questa configurazione, connettere due porte TAP alle porte di monitoraggio 1 e 2 del Flow Sensor.



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 di una direzione di trasmissione.

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.



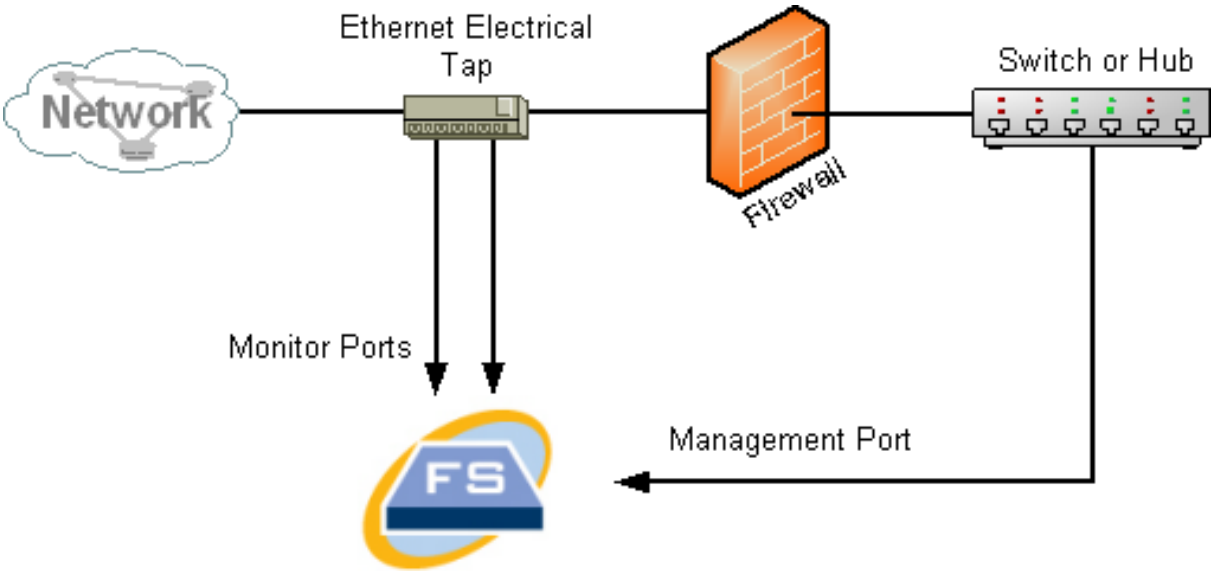
Se la connessione tra le reti monitorate è una connessione ottica, il Flow Sensor è connesso a due splitter ottici. La porta di gestione è connessa allo switch della rete monitorata o a un altro switch o hub.

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 Stealthwatch 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.

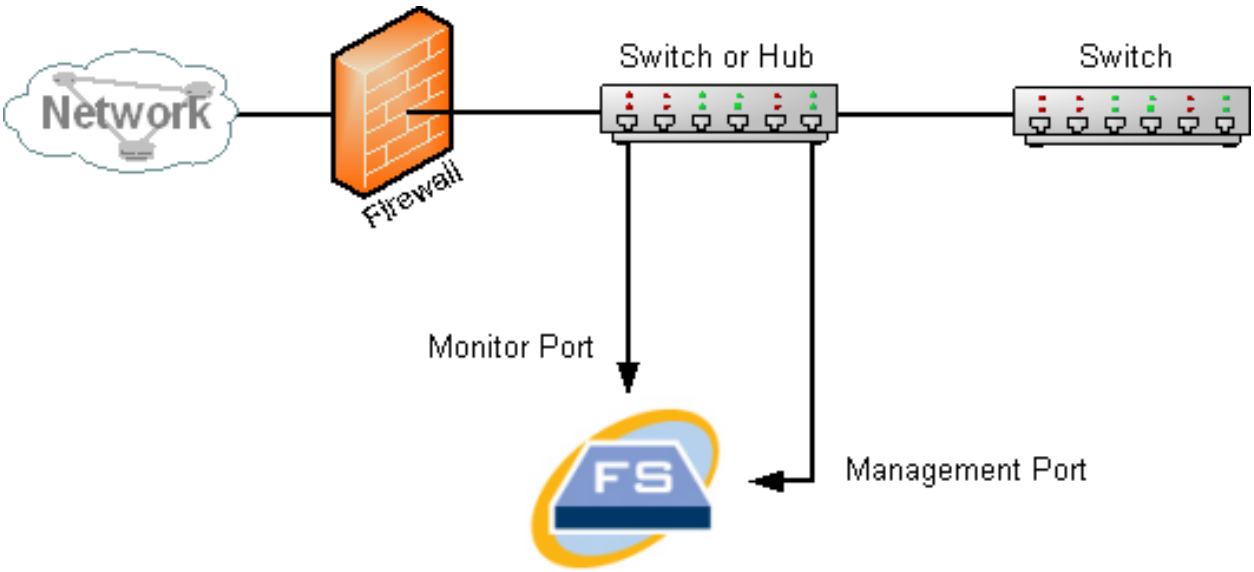
Nell'esempio riportato di seguito viene illustrato l'uso di una TAP Ethernet elettrica. La porta di gestione deve essere connessa allo switch o all'hub della rete monitorata. Questa configurazione è simile a quella che prevede il monitoraggio del traffico da e verso la rete.



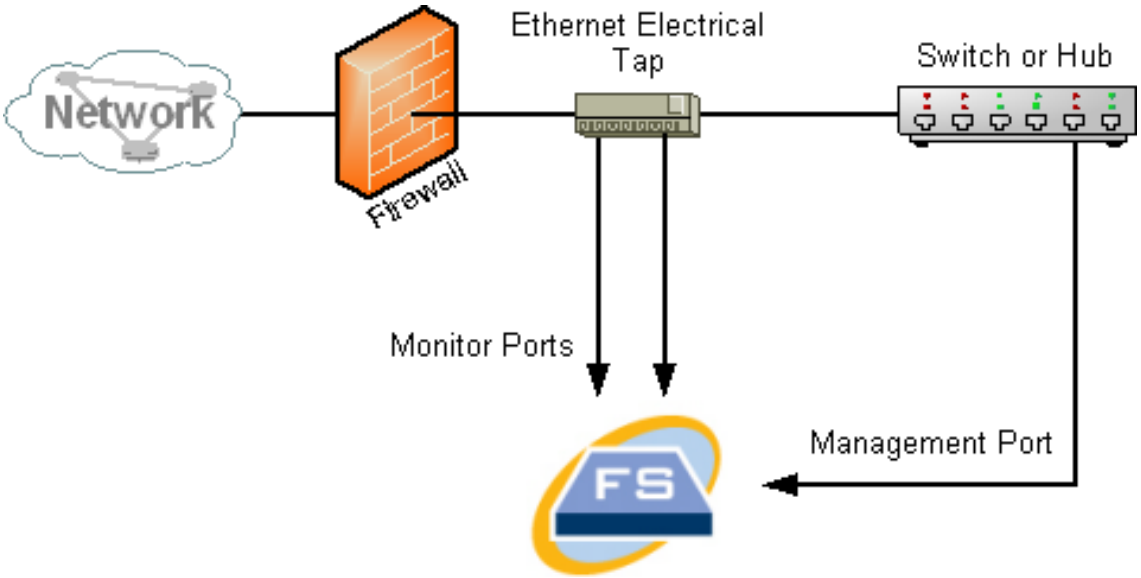
Se il firewall esegue il NAT (network address translation), è possibile osservare solo gli indirizzi presenti sul firewall.

Posizionamento del Flow Sensor all'interno del firewall

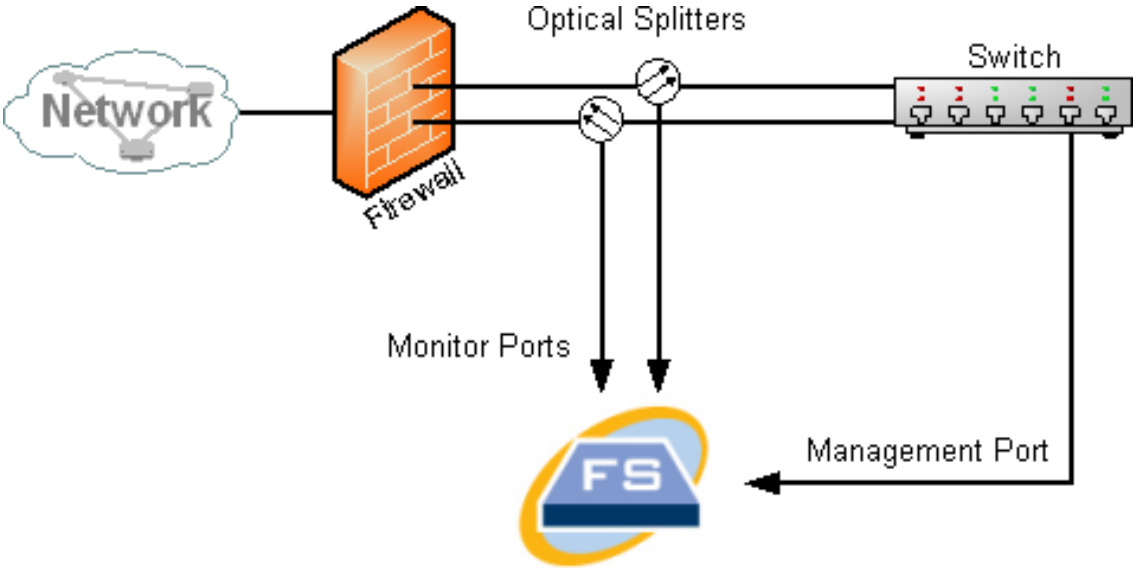
Per monitorare il traffico tra reti interne e firewall, il Flow Sensor deve essere in grado di accedere a tutto il traffico tra il firewall e le reti interne. Per ottenere questo risultato, è necessario configurare una porta di mirroring che rifletta la connessione al firewall sullo switch principale. 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 porta 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.



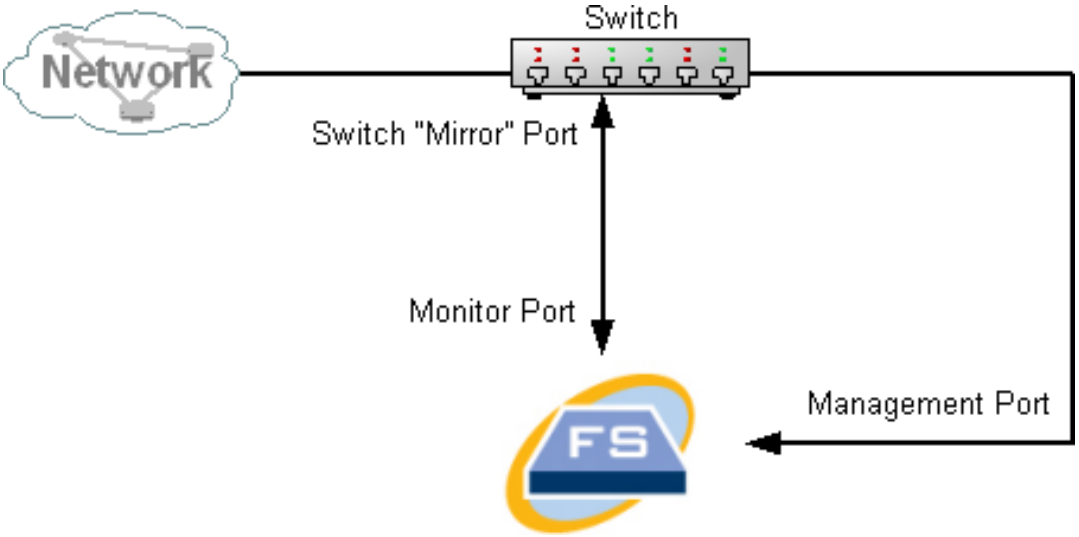
Di seguito viene illustrata una configurazione con splitter ottico.



Porte SPAN

È anche possibile collegare il Flow Sensor 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 ripeta i pacchetti trasmessi da e verso 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 illustra in che modo è possibile ottenere questa configurazione collegando la propria rete a Stealthwatch Flow Sensor tramite la porta di gestione.



In questa configurazione, è necessario configurare una porta dello switch (denominata anche porta di mirroring) per ripetere tutto il traffico da e verso l'host di interesse alla

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 da e verso la rete di interesse e altre reti. In questo caso, una rete può essere composta da alcuni o 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 più logiche che 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 a, da e all'interno della rete di interesse, oltre ad 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.

Installazione

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**
- **Modifica delle informazioni predefinite**

Montaggio dell'appliance

Le appliance Stealthwatch 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 Stealthwatch:

- 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.

Per informazioni sulle specifiche di ciascuna appliance, fare riferimento alle schede tecniche di Stealthwatch.

> Tutti i componenti hardware di Cisco x210 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.

> 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 i 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. Continuare alla sezione **Modifica delle informazioni predefinite**.

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. Continuare alla sezione **Modifica delle informazioni predefinite**.

Modifica delle informazioni predefinite

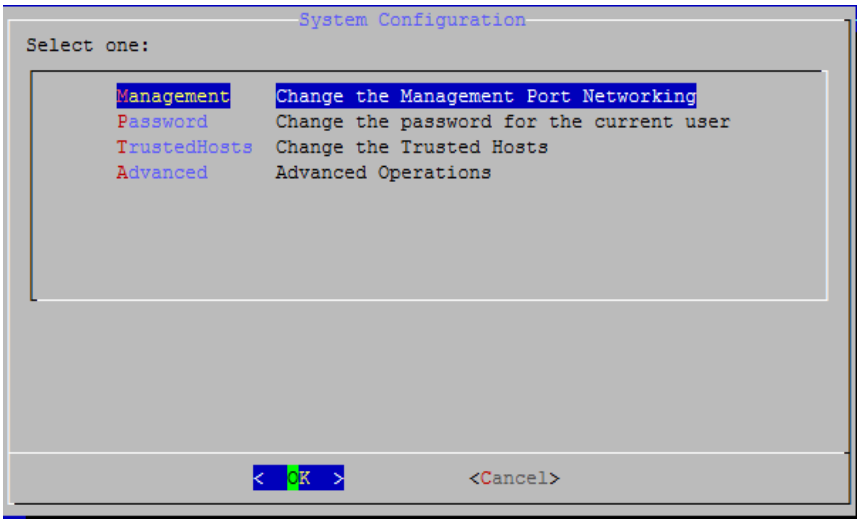
Dopo essersi collegati all'appliance, configurare gli indirizzi IP e modificare le password utente.

Modifica degli indirizzi IP predefiniti

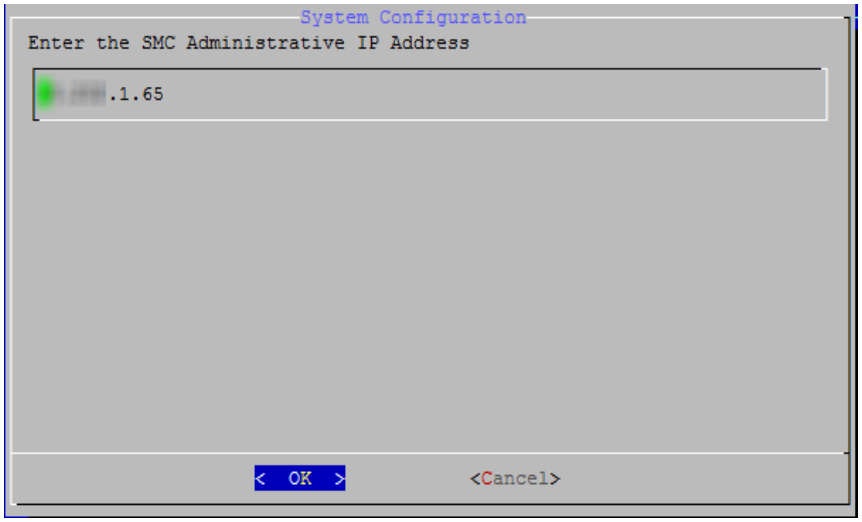
Le appliance dispongono già di indirizzi IP predefiniti ma è necessario configurarli per la propria rete.

1. Accedere al programma di configurazione del sistema:
   - Digitare **sysadmin**, quindi premere **Invio**.
   - Quando viene visualizzato il prompt della password, digitare **lan1cope**, quindi premere **Invio**.
   - Al prompt successivo, digitare **SystemConfig**, quindi premere **Invio**.

     Viene visualizzato il menu di configurazione del sistema.

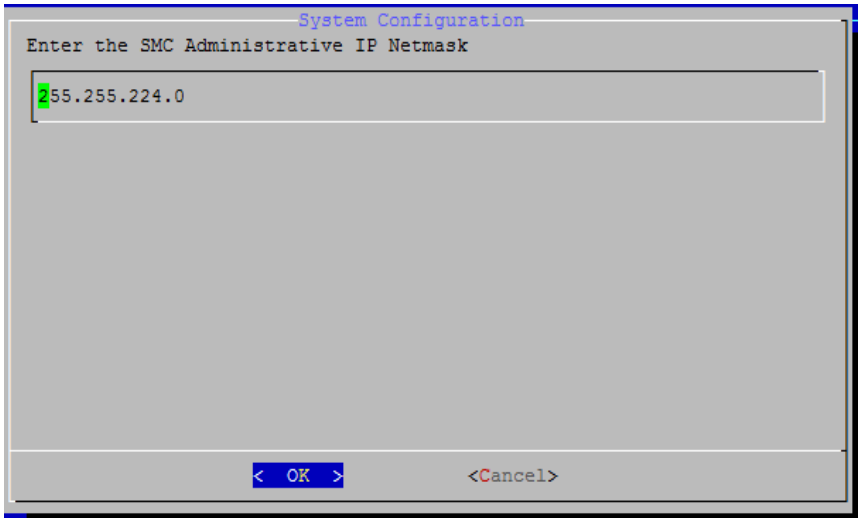


2. Selezionare **Management** (Gestione), quindi premere **Invio**. Viene visualizzata la pagina dell'indirizzo IP.



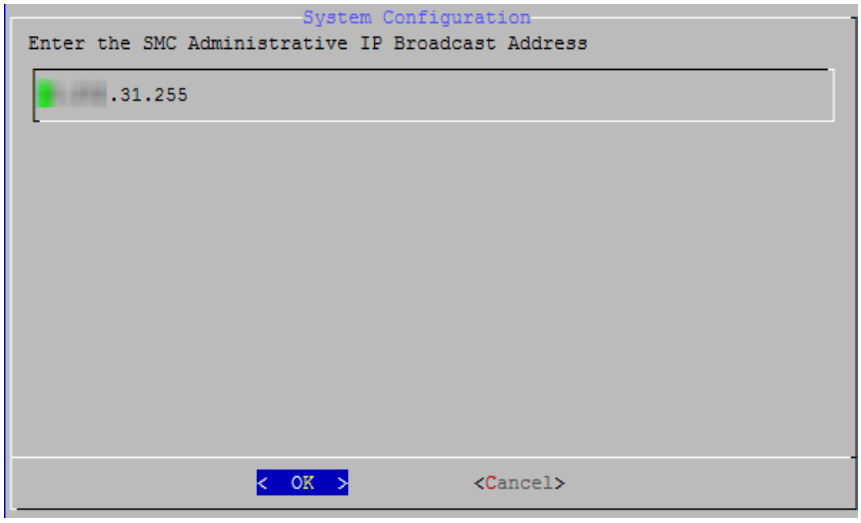
3. Digitare un nuovo indirizzo IP in base all'ambiente in uso. Selezionare **OK**, quindi premere **Invio** per continuare.

   Viene visualizzata la pagina della netmask IP con il valore predefinito.



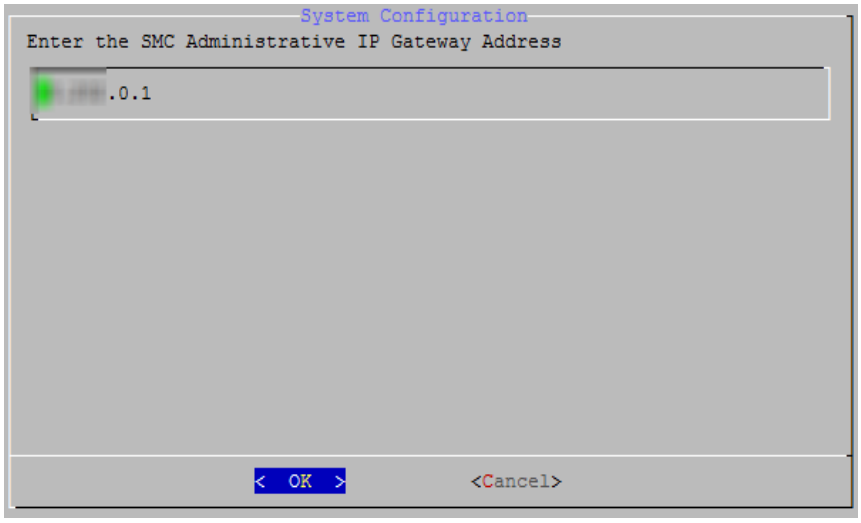
4. Accettare il valore predefinito o immettere un nuovo indirizzo Netmask IP in base all'ambiente in uso. Selezionare **OK**, quindi premere **Invio** per continuare.

Viene visualizzata la pagina dell'indirizzo di broadcast.



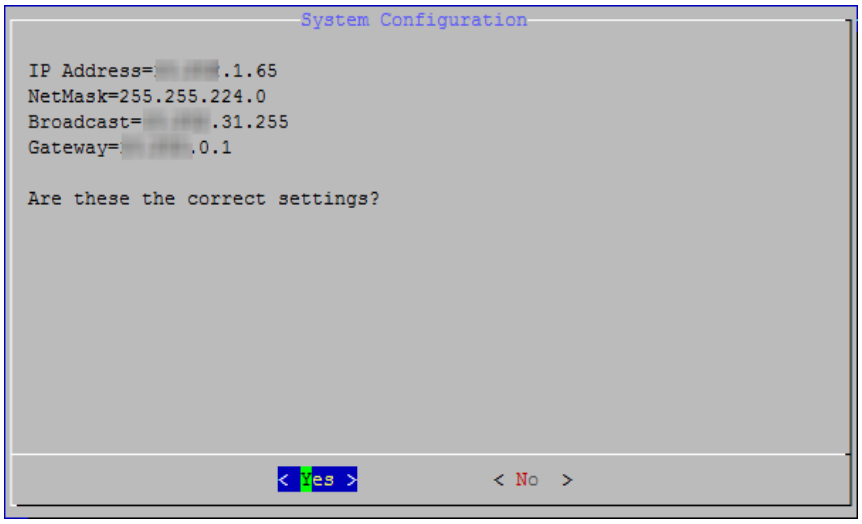
5. Accettare il valore predefinito o immetterne uno nuovo in base all'ambiente in uso. Selezionare **OK**, quindi premere **Invio** per continuare.

   Viene visualizzata la pagina dell'indirizzo gateway con l'indirizzo IP del server gateway predefinito.



6. Accettare il valore predefinito o immetterne uno nuovo in base all'ambiente in uso. Selezionare **OK**, quindi premere **Invio** per continuare.

Viene visualizzata la pagina di conferma.



7. Riesaminare le informazioni. Le impostazioni sono corrette?

- In caso affermativo, selezionare **Yes** (Sì), quindi premere **Invio** per continuare. Il sistema viene riavviato e vengono implementate le modifiche. Al termine, viene visualizzata la pagina di accesso.
- In caso contrario, selezionare **No** per apportare le modifiche. Viene visualizzata la pagina dell'indirizzo IP per poter apportare le modifiche. Una volta apportate le modifiche e aver confermato le impostazioni, viene visualizzata la pagina di riavvio. Premere **Invio** per implementare le modifiche.***La pagina di riavvio non viene visualizzata.***

8. Continuare alla sezione **Modifica della password utente Sysadmin**.

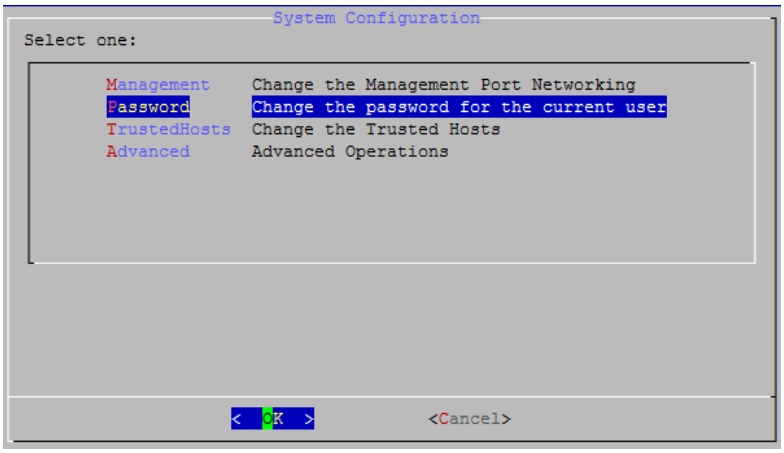
Modifica della password utente Sysadmin

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

Prima di avviare la procedura, accedere come **sysadmin**.

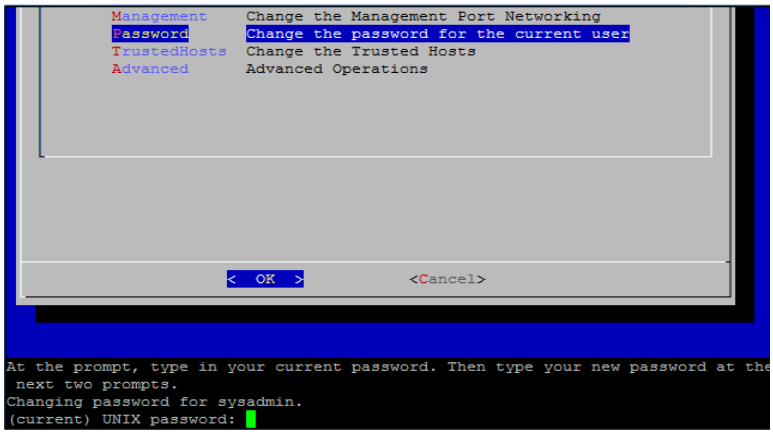
Per modificare la password sysadmin:

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



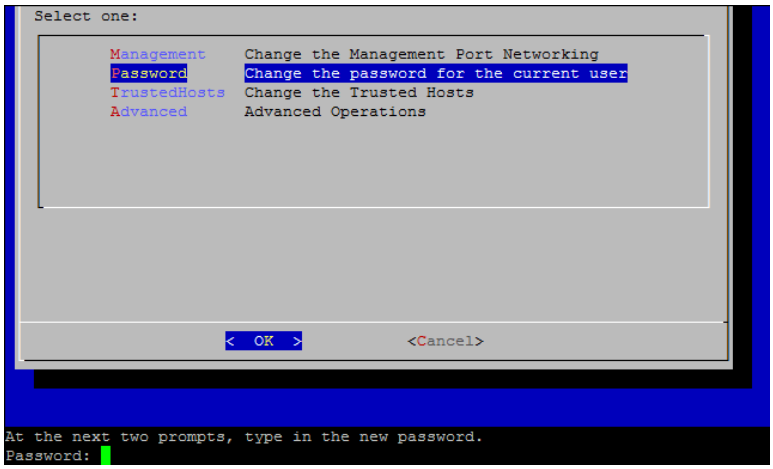
   Se l'elenco predefinito degli host fidati è stato modificato, verificare che ciascuna appliance Stealthwatch presente nella struttura sia inclusa. In caso contrario, le appliance non potranno comunicare tra di loro.

   Sotto il menu viene visualizzato un prompt per la password corrente.



2. Digitare la password corrente e premere **Invio**.

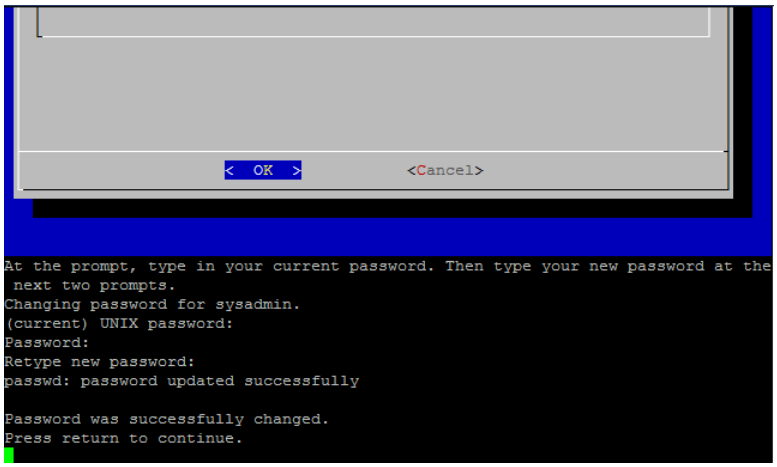
Viene visualizzato il prompt per una nuova password.



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**.

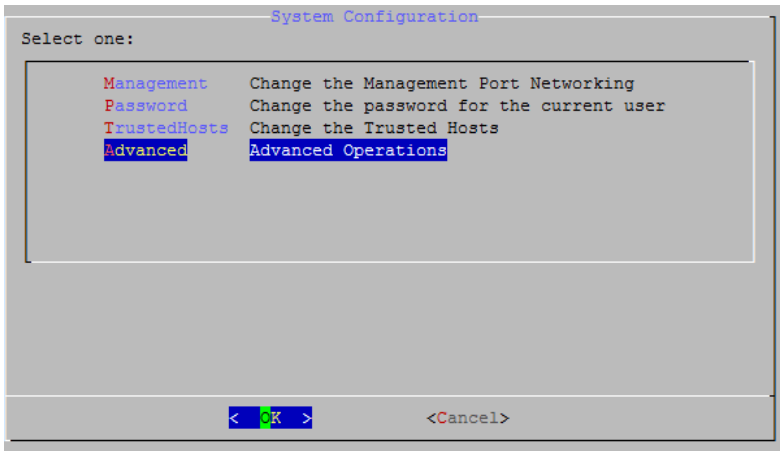


5. Una volta accettata la password, premere **Invio** di nuovo per tornare al menu di configurazione del sistema.
6. Continuare alla sezione **Modifica della password utente root**.

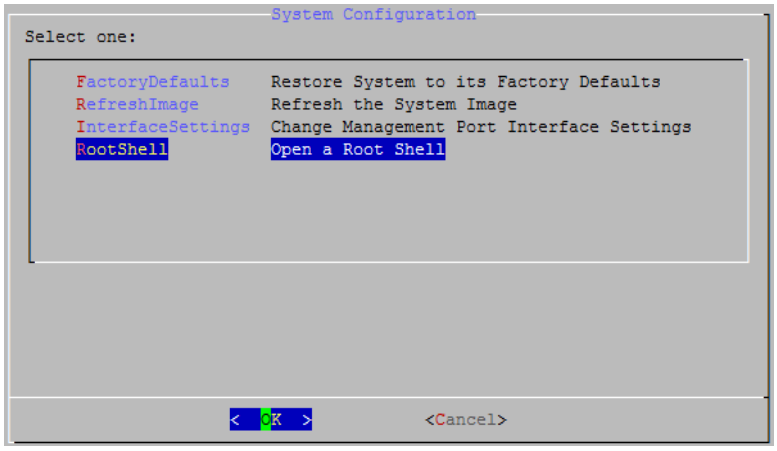
Modifica della password utente root

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

1. Andare alla shell root.

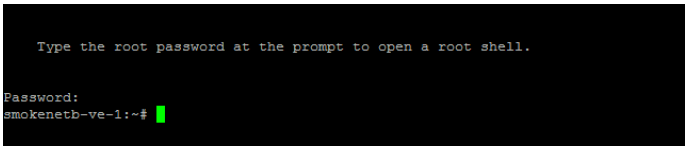


2. Nel menu di configurazione del sistema, selezionare **Advanced** (Avanzate) e premere **Invio**. Viene visualizzato il menu Advanced (Avanzate).

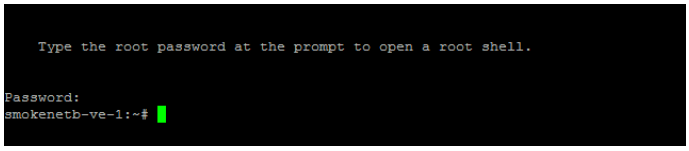


3. Selezionare **RootShell**, quindi premere **Invio**.

   Viene visualizzato il prompt per la password root.



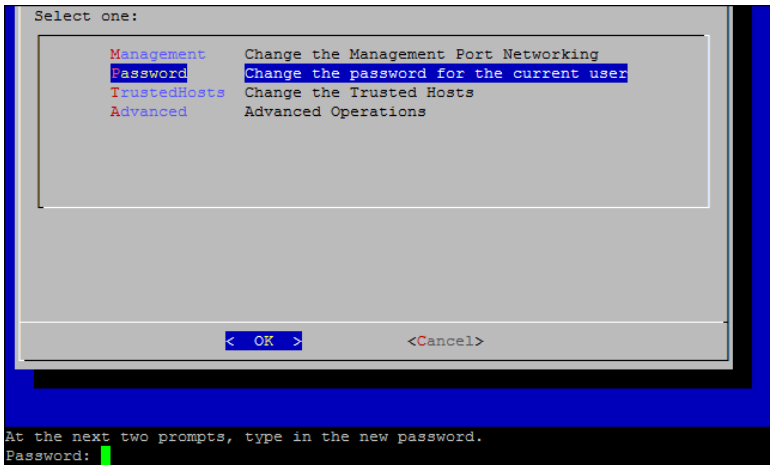
4. Digitare la password root corrente e premere **Invio**. Viene visualizzato il prompt per la shell root.



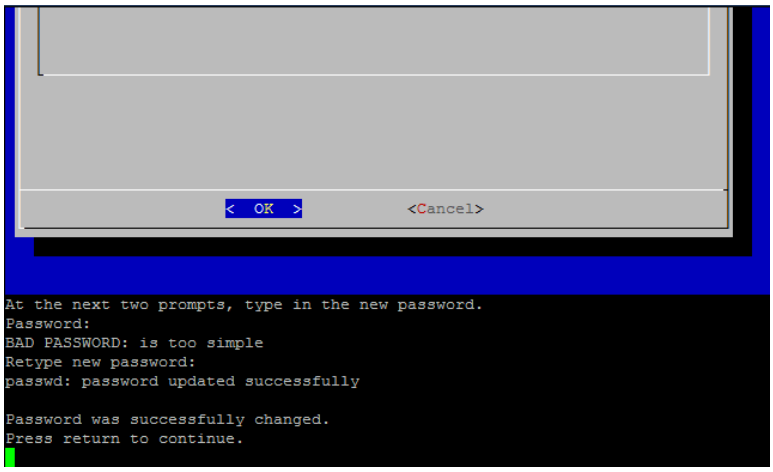
5. Digitare **SystemConfig**, quindi premere **Invio**.

   In questo modo, si torna al menu di configurazione del sistema da dove è possibile modificare la password root.

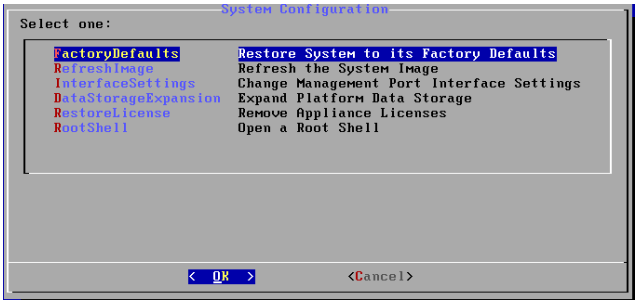
6. Selezionare **Password**, quindi premere **Invio**. Sotto il menu viene visualizzato il prompt per la password.



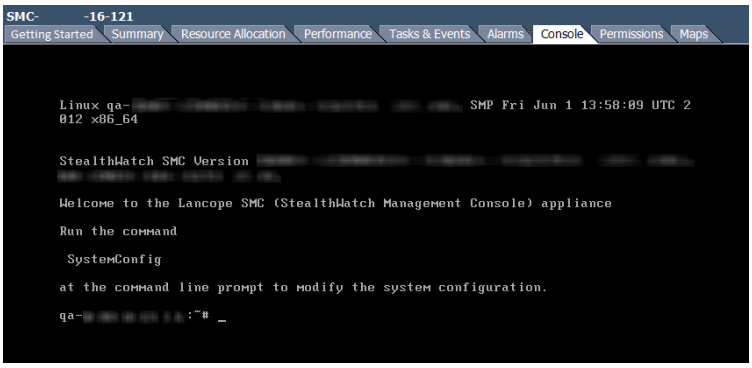
7. Digitare la nuova password root e premere **Invio**. Viene visualizzato un secondo prompt.



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.

Configurazione dell'appliance

A questo punto è possibile configurare l'appliance. Per configurare l'appliance, consultare la **guida di installazione e configurazione Stealthwatch** adeguata alla versione di software interessata. La serie x210 è compatibile con le versioni software Stealthwatch 7.x.

Copyright Information