Configurazione delle interfacce Firepower Threat Defense in modalità di routing

Sommario

Introduzione

In questo documento viene descritta la configurazione, la verifica e il funzionamento di un'interfaccia a coppia inline su un accessorio Firepower Threat Defense (FTD).

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- ASA5512-X - codice FTD 6.1.0.x
- Firepower Management Center (FMC) - codice 6.1.0.x

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

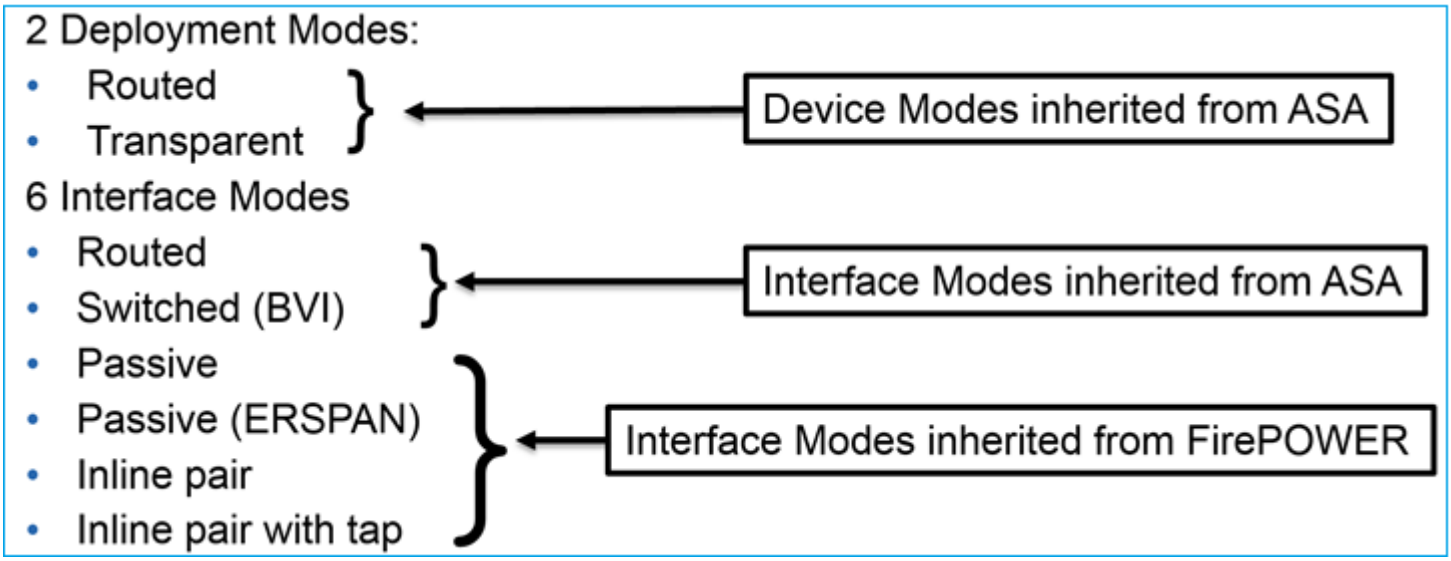
Prodotti correlati

Il presente documento può essere utilizzato anche per le seguenti versioni hardware e software:

- ASA5506-X, ASA5506W-X, ASA5506H-X, ASA5508-X, ASA5516-X
- ASA5512-X, ASA5515-X, ASA5525-X, ASA5545-X, ASA5555-X
- FPR2100, FPR4100, FPR9300
- VMware (ESXi), Amazon Web Services (AWS), Kernel-based Virtual Machine (KVM)
- Codice software FTD 6.2.x e versioni successive

Premesse

Firepower Threat Defense (FTD) fornisce due modalità di distribuzione e sei modalità di interfaccia, come mostrato in questa immagine:



Nota: è possibile utilizzare più modalità di interfaccia su un unico accessorio FTD.

Panoramica di alto livello delle diverse modalità di installazione FTD e interfaccia:

Interfaccia FTD modalità	Modalità di distribuzione FTD	Descrizione	Il traffico può essere interrotto
Stesura	Stesura	Controlli completi del motore LINA e del motore Snort	Sì
Commutato	Trasparente	Controlli completi del motore LINA e del motore Snort	Sì

Coppia inline	Routed o Transparent	Controlli parziali del motore LINA e completi del motore Snort	Sì
Coppia inline con tap	Routed o Transparent	Controlli parziali del motore LINA e completi del motore Snort	No
Passivo	Routed o Transparent	Controlli parziali del motore LINA e completi del motore Snort	No
Passivo (ERSPAN)	Stesura	Controlli parziali del motore LINA e completi del motore Snort	No

Configurazione

Esempio di rete

Configurazione di un'interfaccia di routing e di una sottointerfaccia

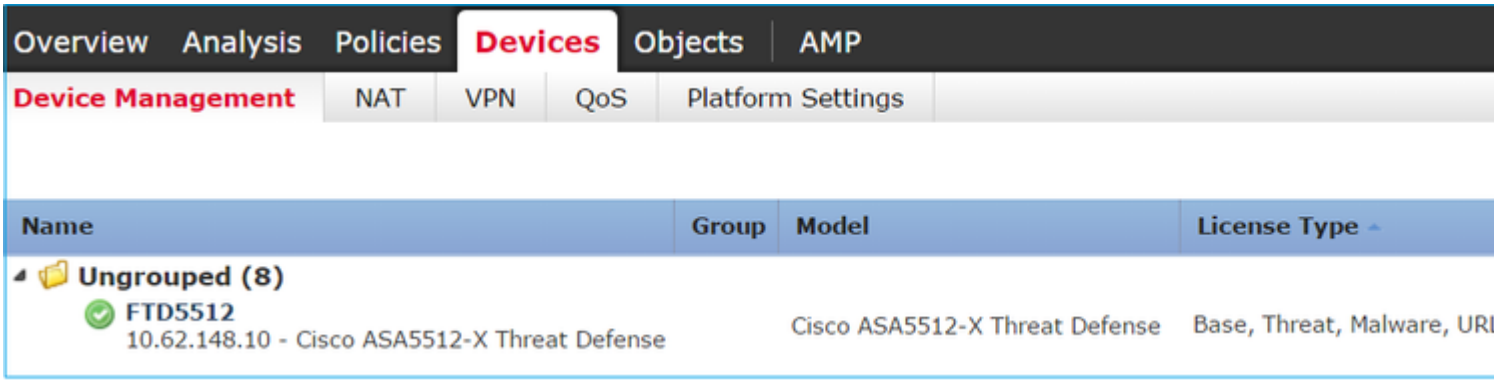
Configurare la sottointerfaccia G0/0.201 e l'interfaccia G0/1 in base ai seguenti requisiti:

Interfaccia	G0/0,201	G0/1
Nome	INTERNO	ESTERNO
Area di sicurezza	AREA_INTERNA	AREA_ESTERNA
Descrizione	INTERNO	ESTERNO
ID sottointerfaccia	201	-
ID VLAN	201	-
IPv4	192.168.201.1/24	192.168.202.1/24
Duplex/velocità	Auto	Auto

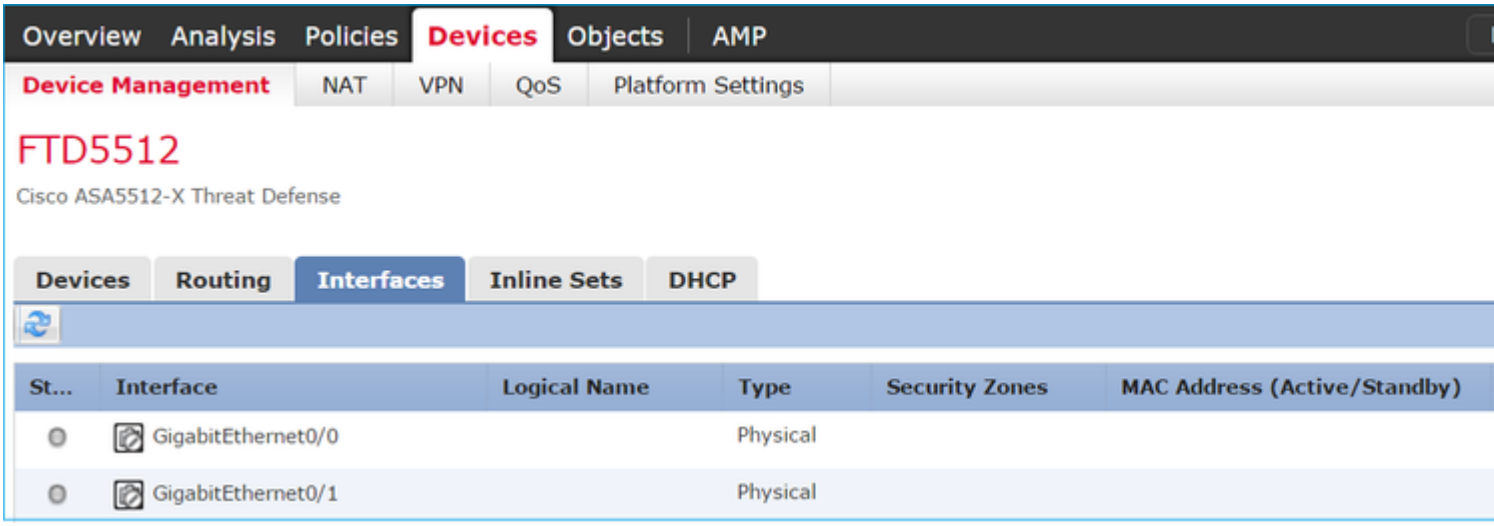
Soluzione

Passaggio 1. Configurazione dell'interfaccia logica

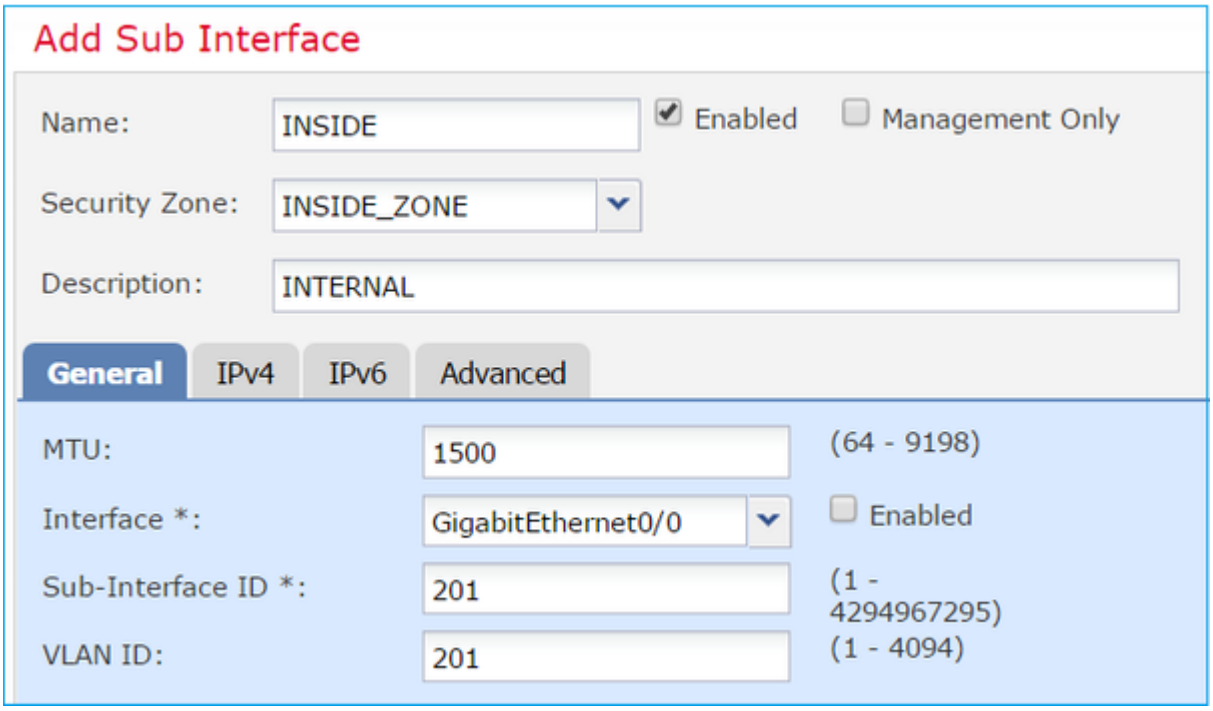
Passare a **Dispositivi > Gestione dispositivi,** selezionare il dispositivo appropriato e fare clic sull'icona **Modifica**:



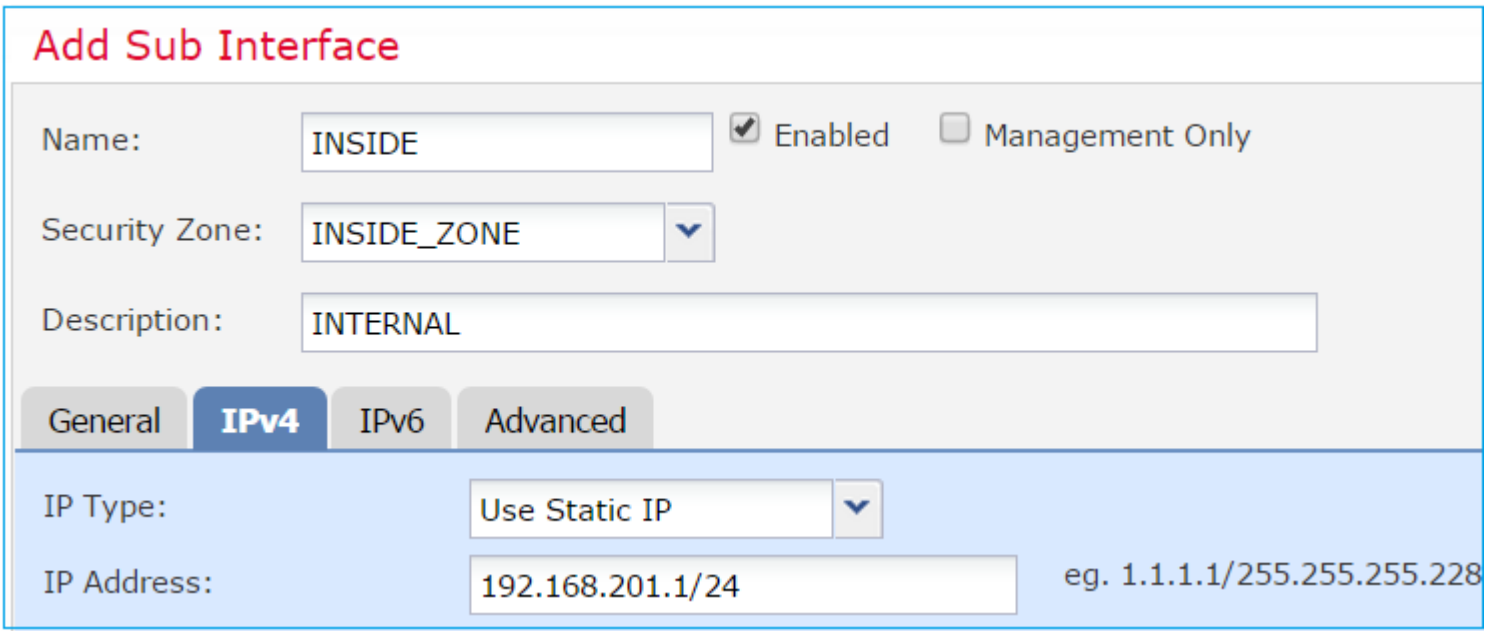
Selezionare **Add Interfaces > Sub Interface**:



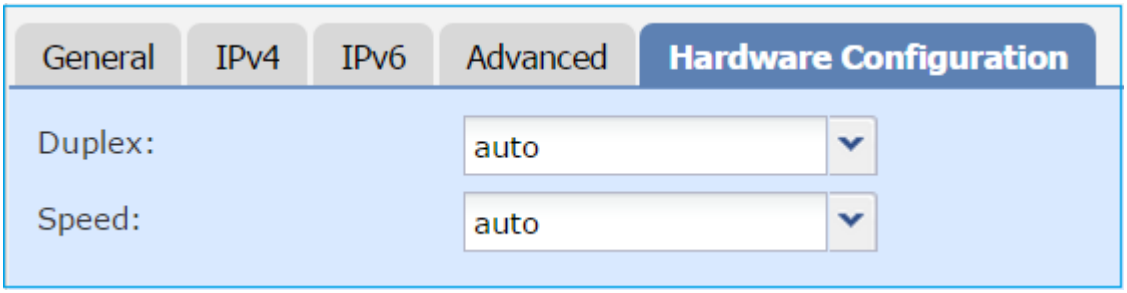
Configurare le impostazioni della sottointerfaccia in base ai requisiti:



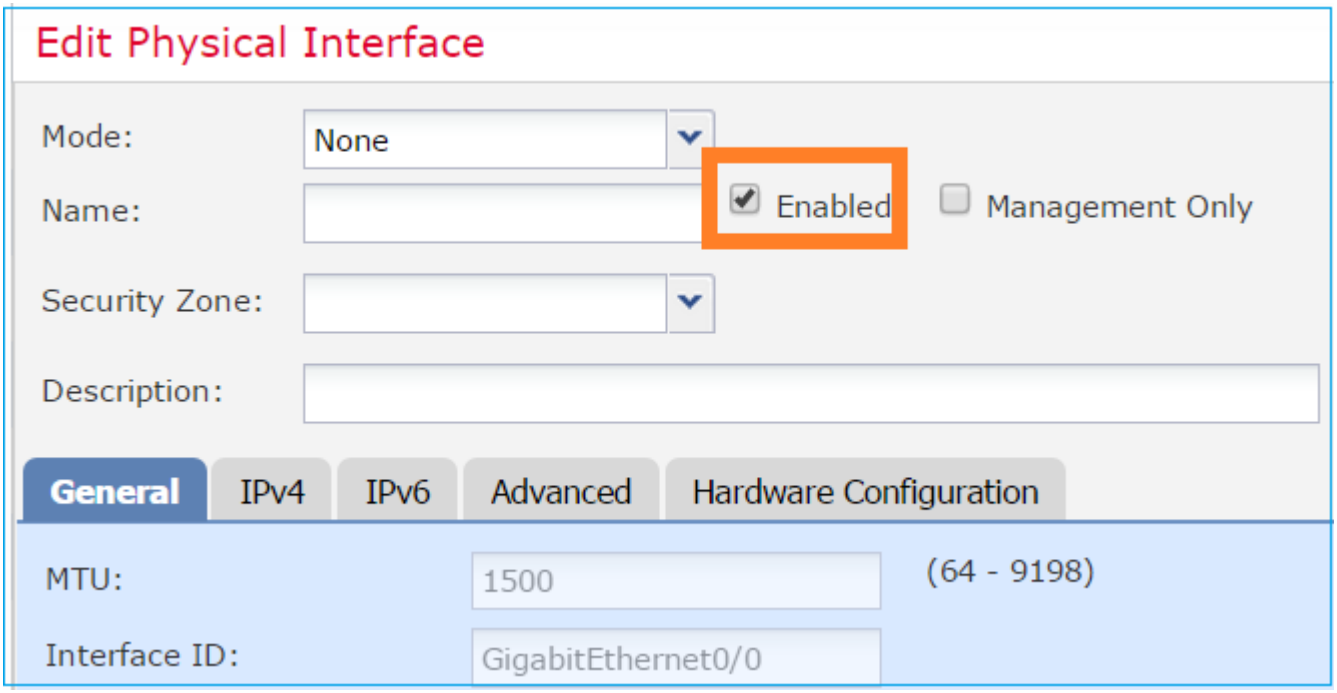
Impostazioni IP interfaccia:



Sotto l'interfaccia fisica (Gigabit Ethernet0/0) specificare le impostazioni duplex e velocità:

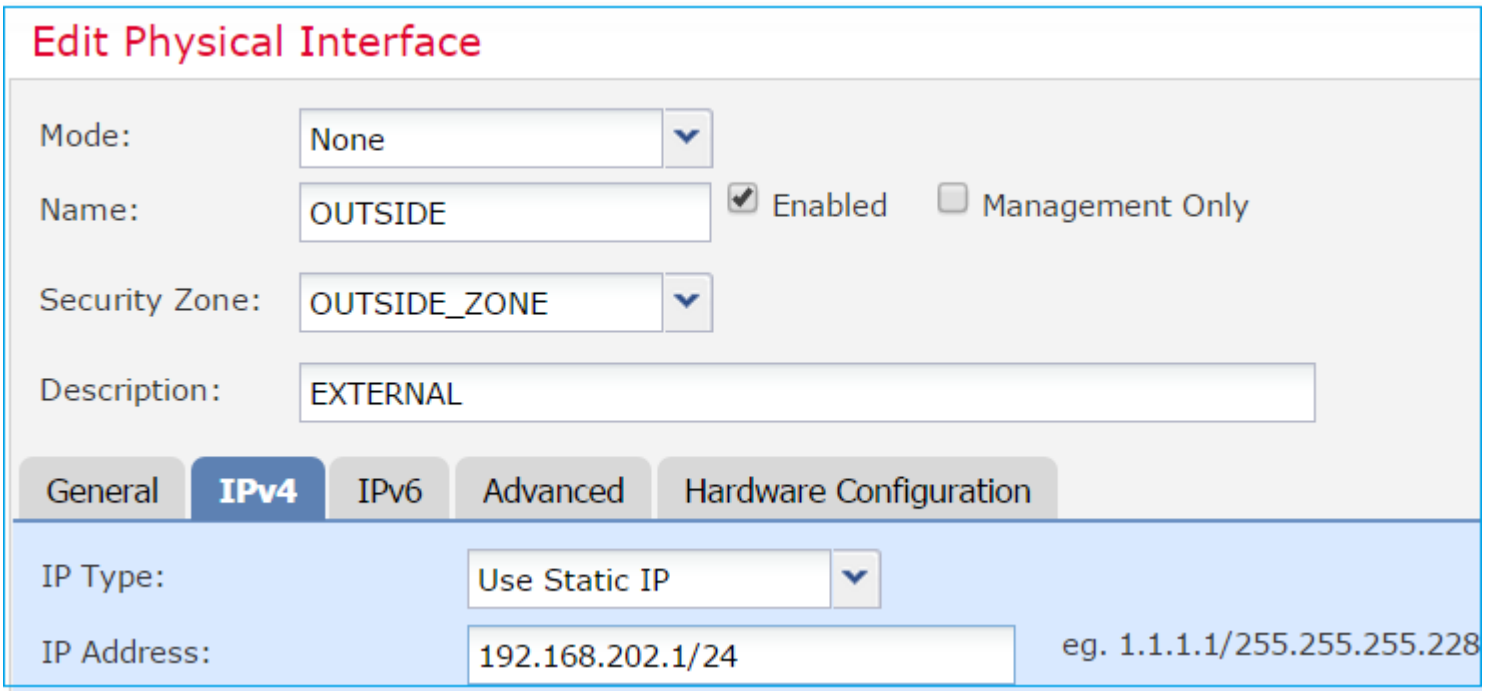


Abilitare l'interfaccia fisica (G0/0 in questo caso):



Passaggio 2. Configurazione dell'interfaccia fisica

Modificare l'interfaccia fisica Gigabit Ethernet 0/1 in base ai requisiti:

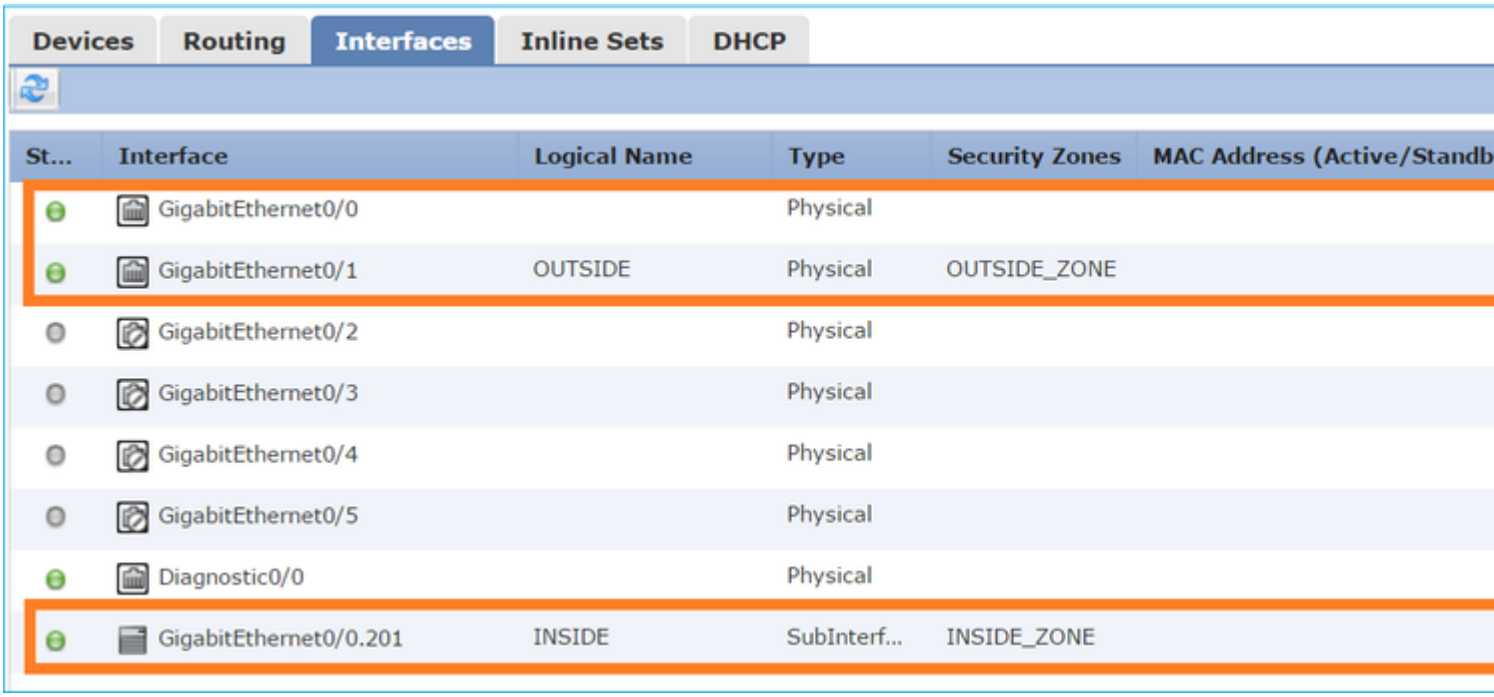


- Per l'interfaccia di routing la modalità è: **Nessuna**
- Il nome è equivalente al **nome** dell'interfaccia ASA **se**
- Su FTD tutte le interfacce hanno il livello di protezione = 0
- **same-security-traffic** non è applicabile su FTD. Il traffico tra le interfacce FTD (inter) e (intra) è consentito per impostazione predefinita

Selezionare **Salva** e **distribuisci.**

Verifica

Dalla GUI del CCP:



St...	Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standb
	GigabitEthernet0/0		Physical		
	GigabitEthernet0/1	OUTSIDE	Physical	OUTSIDE_ZONE	
	GigabitEthernet0/2		Physical		
	GigabitEthernet0/3		Physical		
	GigabitEthernet0/4		Physical		
	GigabitEthernet0/5		Physical		
	Diagnostic0/0		Physical		
	GigabitEthernet0/0.201	INSIDE	SubInterf...	INSIDE_ZONE	

Dalla CLI FTD:

<#root>

>

show interface ip brief

```
Interface                  IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0         unassigned      YES unset  up                    up

GigabitEthernet0/0.201     192.168.201.1   YES manual up                    up
GigabitEthernet0/1         192.168.202.1   YES manual up                    up

GigabitEthernet0/2         unassigned      YES unset  administratively down down
GigabitEthernet0/3         unassigned      YES unset  administratively down down
GigabitEthernet0/4         unassigned      YES unset  administratively down down
GigabitEthernet0/5         unassigned      YES unset  administratively down down
Internal-Control0/0        127.0.1.1       YES unset  up                    up
Internal-Data0/0           unassigned      YES unset  up                    up
Internal-Data0/1           unassigned      YES unset  up                    up
Internal-Data0/2           169.254.1.1     YES unset  up                    up
Management0/0              unassigned      YES unset  up                    up
```

<#root>

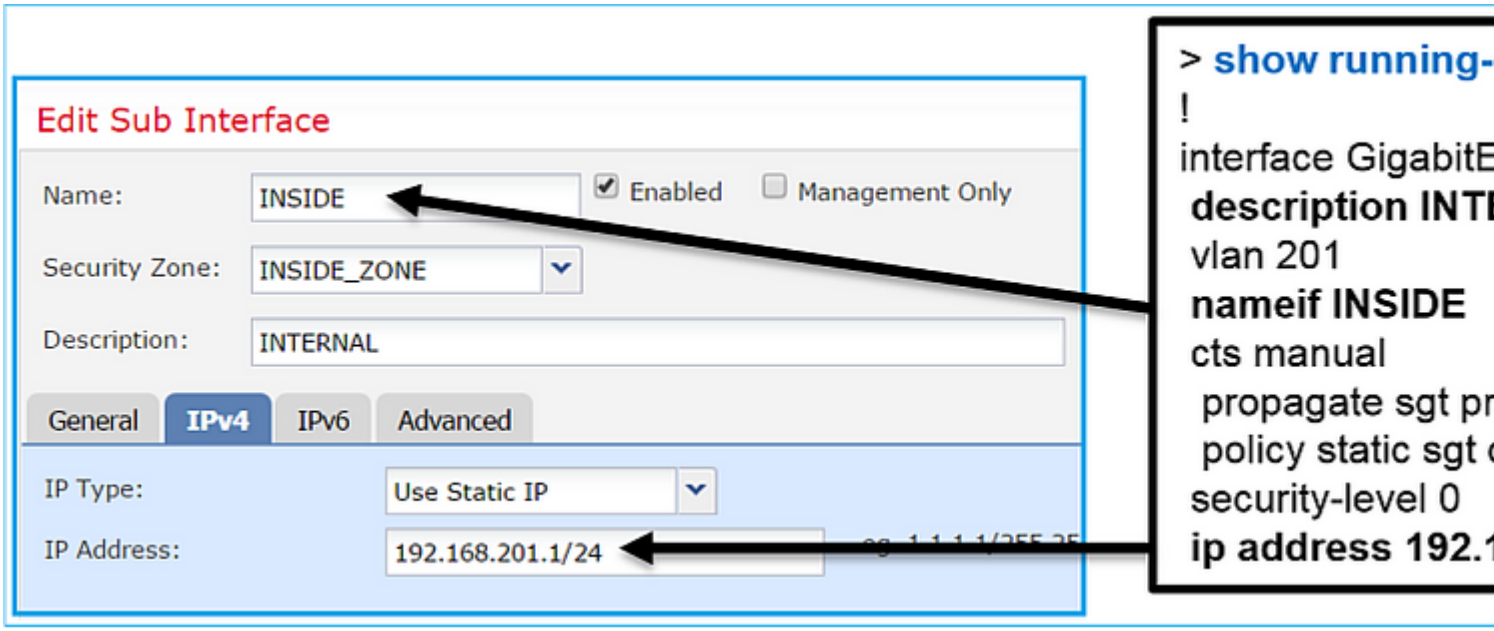
>

show ip

```
System IP Addresses:
Interface                  Name                 IP address      Subnet mask     Method
GigabitEthernet0/0.201     INSIDE               192.168.201.1   255.255.255.0   manual
GigabitEthernet0/1         OUTSIDE              192.168.202.1   255.255.255.0   manual
Current IP Addresses:
Interface                  Name                 IP address      Subnet mask     Method

GigabitEthernet0/0.201     INSIDE               192.168.201.1   255.255.255.0   manual
GigabitEthernet0/1         OUTSIDE              192.168.202.1   255.255.255.0   manual
```

Correlazione tra GUI FMC e CLI FTD:



<#root>

>

show interface g0/0.201

Interface GigabitEthernet0/0.201

"

INSIDE

",

is up, line protocol is up

  Hardware is i82574L rev00, BW 1000 Mbps, DLY 10 usec

VLAN identifier 201

Description: INTERNAL

        MAC address a89d.21ce.fdea, MTU 1500

IP address 192.168.201.1, subnet mask 255.255.255.0

  Traffic Statistics for "INSIDE":

```
        1 packets input, 28 bytes
        1 packets output, 28 bytes
        0 packets dropped
>

show interface g0/1

Interface GigabitEthernet0/1 "OUTSIDE", is up, line protocol is up

  Hardware is i82574L rev00, BW 1000 Mbps, DLY 10 usec


 Auto-Duplex(Full-duplex), Auto-Speed(1000 Mbps)

        Input flow control is unsupported, output flow control is off


Description: EXTERNAL

        MAC address a89d.21ce.fde7, MTU 1500


IP address 192.168.202.1, subnet mask 255.255.255.0

        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 pause input, 0 resume input
        0 L2 decode drops
        1 packets output, 64 bytes, 0 underruns
        0 pause output, 0 resume output
        0 output errors, 0 collisions, 12 interface resets
        0 late collisions, 0 deferred
        0 input reset drops, 0 output reset drops
        input queue (blocks free curr/low): hardware (511/511)
        output queue (blocks free curr/low): hardware (511/511)
  Traffic Statistics for "OUTSIDE":
        0 packets input, 0 bytes
        0 packets output, 0 bytes
        0 packets dropped
      1 minute input rate 0 pkts/sec,  0 bytes/sec
      1 minute output rate 0 pkts/sec,  0 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  0 bytes/sec
      5 minute output rate 0 pkts/sec,  0 bytes/sec
      5 minute drop rate, 0 pkts/sec
>
```

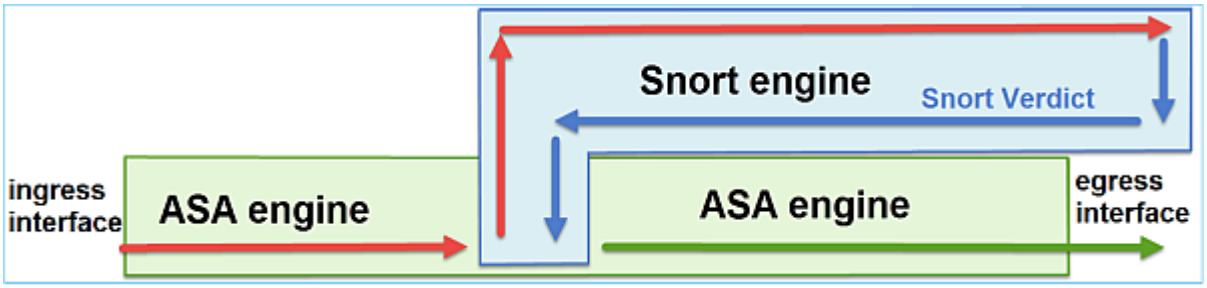
Operazione interfaccia ciclo FTD

Verificare il flusso del pacchetto FTD quando le interfacce di routing sono in uso.

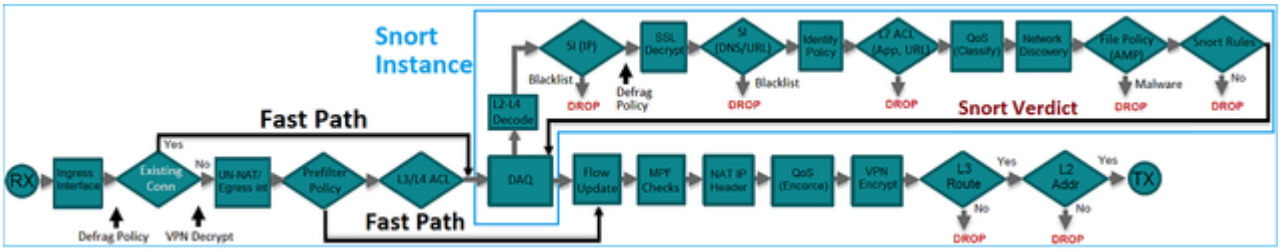
Soluzione

Panoramica dell'architettura FTD

Panoramica generale del piano dati FTD:



L'immagine mostra alcuni dei controlli eseguiti all'interno di ciascun motore:



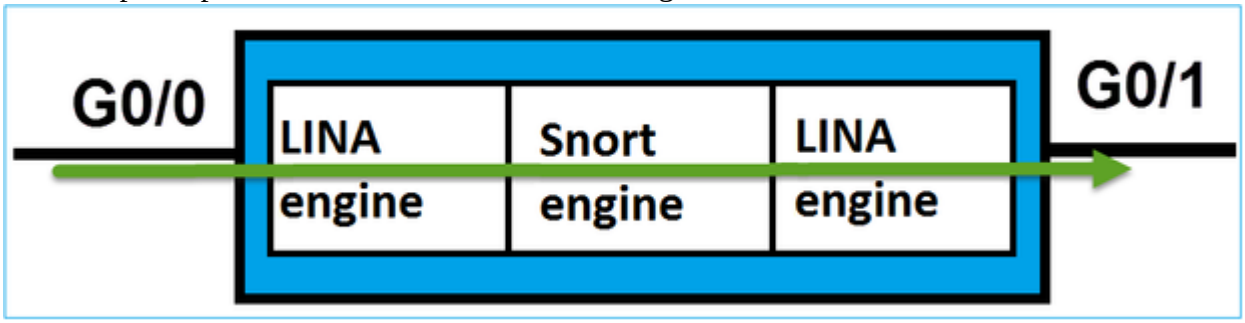
Punti chiave

- I controlli inferiori corrispondono al percorso dei dati del motore LINA FTD
- I controlli all'interno della casella blu corrispondono all'istanza del motore Snort FTD

Panoramica sull'interfaccia di routing FTD

- Disponibile solo in Distribuzione **con routing**
- **Implementazione** tradizionale **del firewall L3**
- Una o più interfacce instradabili fisiche o logiche (VLAN)
- Consente di configurare funzionalità quali i protocolli NAT o Dynamic Routing
- I pacchetti vengono inoltrati in base alla **ricerca route** e l'hop successivo viene risolto in base alla **ricerca ARP**
- Traffico effettivo **può essere eliminato**
- I controlli **completi del motore LINA** vengono applicati insieme ai controlli **completi del motore Snort**

L'ultimo punto può essere visualizzato nel modo seguente:



Verifica

Traccia un pacchetto sull'interfaccia di routing FTD

Esempio di rete

Utilizzare packet-tracer con i seguenti parametri per visualizzare i criteri applicati:

Interfaccia di ingresso	INTERNO
Protocollo/servizio	porta TCP 80
IP di origine	192.168.201.100
IP di destinazione	192.168.202.100

Soluzione

Quando si usa un'interfaccia di routing, il pacchetto viene elaborato in modo simile all'interfaccia ASA classica. Controlli quali Ricerca route, Modular Policy Framework (MPF), NAT, Ricerca ARP e così via vengono eseguiti nel percorso dati del motore LINA. Inoltre, se la Policy di controllo degli accessi lo richiede, il pacchetto viene ispezionato dal motore Snort (una delle istanze Snort), dove viene generato un verdetto che viene restituito al motore LINA:

<#root>

>

packet-tracer input INSIDE tcp 192.168.201.100 11111 192.168.202.100 80

Phase: 1

Type: ROUTE-LOOKUP

Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:

found next-hop 192.168.202.100 using egress ifc OUTSIDE

Phase: 2

Type: ACCESS-LIST

Subtype: log
Result: ALLOW
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced permit ip any any rule-id 268437505
access-list CSM_FW_ACL_ remark rule-id 268437505: ACCESS POLICY: FTD5512 - Default/1
access-list CSM_FW_ACL_ remark rule-id 268437505: L4 RULE: DEFAULT ACTION RULE

Additional Information:

This packet will be sent to snort for additional processing where a verdict will be reached

Phase: 3

Type: CONN-SETTINGS

Subtype:
Result: ALLOW
Config:

class-map class-default

match any

policy-map global_policy

class class-default

set connection advanced-options UM_STATIC_TCP_MAP

service-policy global_policy global

Additional Information:

Phase: 4

Type: NAT

Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 5
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 6
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 7
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 8
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 11336, packet dispatched to next module

Result:

input-interface: INSIDE

input-status: up
input-line-status: up

output-interface: OUTSIDE

```
output-status: up
output-line-status: up
Action: allow

>
```

Nota: nella fase 4 il pacchetto viene confrontato con una mappa TCP chiamata UM_STATIC_TCP_MAP. Questa è la mappa TCP predefinita su FTD.

<#root>

```
firepower#
```

show run all tcp-map

```
!
tcp-map UM_STATIC_TCP_MAP
  no check-retransmission
  no checksum-verification
  exceed-mss allow
  queue-limit 0 timeout 4
  reserved-bits allow
  syn-data allow
  synack-data drop
  invalid-ack drop
  seq-past-window drop
  tcp-options range 6 7 allow
  tcp-options range 9 18 allow
  tcp-options range 20 255 allow
  tcp-options selective-ack allow
  tcp-options timestamp allow
  tcp-options window-scale allow
  tcp-options mss allow
  tcp-options md5 clear
  ttl-evasion-protection
  urgent-flag allow
  window-variation allow-connection
!
>
```

Informazioni correlate

- Guida alla configurazione di Cisco Firepower Threat Defense per Firepower Device Manager, versione 6.1
- Installazione e aggiornamento di Firepower Threat Defense sui dispositivi ASA 55xx-X
- Cisco Secure Firewall Threat Defense
- Supporto tecnico e download Cisco

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).