

Come confrontare i criteri di Protezione accesso alla rete sui dispositivi Firepower

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Verifica configurazione di Protezione accesso alla rete](#)

Introduzione

In questo documento viene descritto come confrontare diversi criteri di analisi della rete (NAP) per dispositivi firepower gestiti da Firepower Management Center (FMC).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenza di Snort open-source
- Firepower Management Center (FMC)
- Firepower Threat Defense (FTD)

Componenti usati

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

- Questo articolo è applicabile a tutte le piattaforme Firepower
- Cisco Firepower Threat Defense (FTD) con software versione 6.4.0
- Firepower Management Center Virtual (FMC) con software versione 6.4.0

Premesse

Lo snort utilizza tecniche di corrispondenza dei pattern per trovare e prevenire gli exploit nei pacchetti di rete. Per fare questo, il motore Snort ha bisogno di pacchetti di rete da preparare in modo tale che questo confronto possa essere fatto. Questo processo viene eseguito con l'aiuto di Protezione accesso alla rete e può essere suddiviso nelle tre fasi seguenti:

- Decodifica
- Normalizzazione
- Pre-elaborazione

Un criterio di analisi della rete elabora i pacchetti in fasi: in primo luogo, il sistema decodifica i pacchetti attraverso i primi tre livelli TCP/IP, quindi continua con la normalizzazione, la pre-elaborazione e il rilevamento delle anomalie di protocollo.

I preprocessori offrono due funzionalità principali:

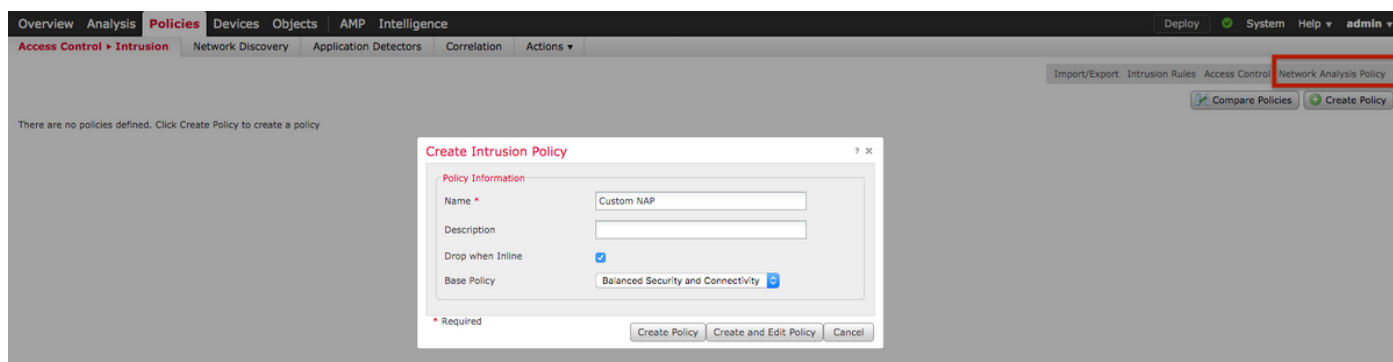
- Normalizzazione del traffico per ulteriori ispezioni
- Identificazione delle anomalie dei protocolli

Nota: alcune regole dei criteri per le intrusioni richiedono alcune opzioni del preprocessore per eseguire il rilevamento

Per informazioni su Snort open-source, visitare il sito <https://www.snort.org/>

Verifica configurazione di Protezione accesso alla rete

Per creare o modificare i criteri di Protezione accesso alla rete di Firepower, selezionare **Criteri FMC > Controllo accesso > Intrusione**, quindi fare clic su **Network Analysis Policy** option nell'angolo in alto a destra, come mostrato nell'immagine:



Network Analysis Policy	Inline Mode	Status	Last Modified
Test1	Yes	No access control policies use this policy Policy not applied on any devices	2019-12-30 02:13:49 Modified by "admin"
Test2*	Yes	You are currently editing this policy No access control policies use this policy Policy not applied on any devices	2019-12-30 02:14:24 Modified by "admin"

Verifica dei criteri di analisi della rete predefiniti

Controllare il criterio predefinito di Analisi rete applicato al criterio di controllo di accesso

Passare a **Criteri > Controllo di accesso** e modificare il punto ACP da verificare. Fare clic sulla scheda **Advanced** (Avanzate) e scorrere verso il basso fino alla sezione **Network Analysis and Intrusion Policies** (Analisi della rete e criteri intrusione).

Il criterio di analisi della rete predefinito associato al provider di servizi di audioconferenza è **Protezione e connettività bilanciate**, come mostrato nell'immagine:

Overview Analysis **Policies** Devices Objects AMP Intelligence

Access Control ▶ Access Control Network Discovery Application Detectors Correlation Actions ▼

Test

Enter Description

Prefilter Policy: [Default Prefilter Policy](#) SSL Policy: [None](#)

Rules Security Intelligence HTTP Responses Logging **Advanced**

General Settings


Maximum URL characters to store in connection events 1024

Allow an Interactive Block to bypass blocking for (seconds) 600

Retry URL cache miss lookup Yes

Network Analysis and Intrusion Policies


Intrusion Policy used before Access Control rule is determined

Intrusion Policy Variable Set 

Network Analysis Rules [No Custom Rules](#) [Network Analysis Policy List](#)

Default Network Analysis Policy

Network Analysis and Intrusion Policies

Intrusion Policy used before Access Control rule is determined 

Intrusion Policy Variable Set

Default Network Analysis Policy

Nota: Non confondere **Protezione e connettività bilanciate** per i criteri di intrusione e **Protezione e connettività bilanciate** per l'analisi della rete. Il primo è per Snort rules, mentre il secondo è per la pre-elaborazione e la decodifica.

Confronta criteri di analisi della rete







I criteri di Protezione accesso alla rete possono essere confrontati con le modifiche apportate e questa funzionalità può aiutare a identificare e risolvere i problemi. È inoltre possibile generare ed esportare contemporaneamente anche report di confronto di Protezione accesso alla rete.

Selezionare **Policy > Controllo accesso > Intrusione**. Quindi, fare clic su **Network Analysis Policy** opzione in alto a destra. Nella pagina dei criteri di Protezione accesso alla rete è possibile visualizzare la scheda **Confronta criteri** nella parte superiore destra, come mostrato nell'immagine:

Deploy ✔ System Help ▼ admin ▼

Object Management Access Control Intrusion

Compare Policies Create Policy

Last Modified		
2019-12-30 01:58:08	Modified by "admin"	  
2019-12-30 01:58:59	Modified by "admin"	  

Il confronto dei criteri di analisi della rete è disponibile in due varianti:

- Tra due diversi criteri di Protezione accesso alla rete
- Tra due diverse revisioni dello stesso criterio di Protezione accesso alla rete

Select Comparison ? ✕

Compare Against

Policy A NAP1one (2019-11-27 14:22:32 by admin) ▾

Policy B NAP1one (2019-11-27 14:22:32 by admin) ▾

Other Policy

Other Revision

OK Cancel

Nella finestra di confronto è disponibile un confronto riga per riga tra due criteri di Protezione accesso alla rete selezionati e lo stesso può essere esportato come report dalla scheda **report di confronto** in alto a destra, come illustrato nell'immagine:

Back Previous Next (Difference 1 of 114) Comparison Report New Comparison

Test1 (2019-12-30 02:13:49 by admin)	Test2 (2019-12-30 02:14:24 by admin)
Policy Information	
Name: Test1	Name: Test2
Modified: 2019-12-30 02:13:49 by admin	Modified: 2019-12-30 02:14:24 by admin
Base Policy: Connectivity Over Security	Base Policy: Maximum Detection
Settings	
Checksum Verification	
ICMP Checksums: Enabled	ICMP Checksums: Disabled
IP Checksums: Enabled	IP Checksums: Drop and Generate Events
TCP Checksums: Enabled	TCP Checksums: Drop and Generate Events
UDP Checksums: Enabled	UDP Checksums: Disabled
DCE/RPC Configuration	
Servers	
default	
SMB Maximum AndX Chain: 3	SMB Maximum AndX Chain: 5
RPC over HTTP Server Auto-Detect Ports: Disabled	RPC over HTTP Server Auto-Detect Ports: 1024-65535
TCP Auto-Detect Ports: Disabled	TCP Auto-Detect Ports: 1024-65535
UDP Auto-Detect Ports: Disabled	UDP Auto-Detect Ports: 1024-65535
SMB File Inspection Depth: 16384	SMB File Inspection Depth:
Packet Decoding	
Detect Invalid IP Options: Disable	Detect Invalid IP Options: Enable
Detect Obsolete TCP Options: Disable	Detect Obsolete TCP Options: Enable
Detect Other TCP Options: Disable	Detect Other TCP Options: Enable
Detect Protocol Header Anomalies: Disable	Detect Protocol Header Anomalies: Enable
DNS Configuration	
Detect Obsolete DNS RR Types: No	Detect Obsolete DNS RR Types: Yes
Detect Experimental DNS RR Types: No	Detect Experimental DNS RR Types: Yes
FTP and Telnet Configuration	
FTP Server	
default	

Per il confronto tra due versioni dello stesso criterio di Protezione accesso alla rete, è possibile scegliere l'opzione di revisione per selezionare l'ID di revisione richiesto, come illustrato nell'immagine:

Select Comparison ? X

Compare Against	Other Revision ▾
Policy	Test1 (2019-12-30 02:13:49 by admin) ▾
Revision A	2019-12-30 02:13:49 by admin ▾
Revision B	2019-12-30 01:58:08 by admin ▾

OK
Cancel

Back

Previous Next (Difference 1 of 13)

Comparison Report New Comparison

Test1 (2019-12-30 02:13:49 by admin)	
Policy Information	
Modified	2019-12-30 02:13:49 by admin
Base Policy	Connectivity Over Security
Settings	
CSP Configuration Disabled	
DCE/RPC Configuration	
Servers	
default	
RPC over HTTP Server Auto-Detect Ports	Disabled
TCP Auto-Detect Ports	Disabled
UDP Auto-Detect Ports	Disabled
HTTP Configuration	
Servers	
default	
Ports	80, 443, 1220, 1741, 2301, 3
Server Flow Depth	300
SSL Configuration	
Ports	443, 465, 563, 636, 989, 992
TCP Stream Configuration	
Servers	
default	
Perform Stream Reassembly on Client Ports	21, 23, 25, 42, 53, 80, 135, 1
Perform Stream Reassembly on Client Services	CYS, DCE/RPC, DNS, , HTTP,
Perform Stream Reassembly on Both Ports	5000, 9800, 9111

Test1 (2019-12-30 01:58:08 by admin)	
Policy Information	
Modified	2019-12-30 01:58:08 by admin
Base Policy	Balanced Security and Connec
Settings	
DCE/RPC Configuration	
Servers	
default	
RPC over HTTP Server Auto-Detect Ports	1024-65535
TCP Auto-Detect Ports	1024-65535
UDP Auto-Detect Ports	1024-65535
HTTP Configuration	
Servers	
default	
Ports	80, 443, 1220, 1741, 2301, 2
Server Flow Depth	500
SSL Configuration	
Ports	443, 465, 563, 636, 989, 992
TCP Stream Configuration	
Servers	
default	
Perform Stream Reassembly on Client Ports	21, 23, 25, 42, 53, 135, 136,
Perform Stream Reassembly on Client Services	CYS, DCE/RPC, DNS, , IMAP,
Perform Stream Reassembly on Both Ports	80, 443, 465, 636, 992, 993,
Perform Stream Reassembly on Both Services	HTTP