PIX/ASA 7.x: Configuratievoorbeeld van FTP/TFTP-services inschakelen

Inhoud

Inleiding
Voorwaarden
Vereisten
Gebruikte componenten
Netwerkdiagram
Verwante producten
Conventies
Achtergrondinformatie
Geavanceerde protocolbehandeling
Basis FTP-toepassingsinspectie configureren
Configuratievoorbeeld
Configuratie FTP-protocolinspectie op niet-standaard TCP-poort
Basis TFTP-toepassingsinspectie configureren
Configuratievoorbeeld
Verifiëren
Problemen oplossen
Probleem: Syntax in Configuration not Work and class-map inspection Error wordt ontvangen
Oplossing
Kan FTPS (FTP over SSL) over ASA niet starten
Gerelateerde informatie

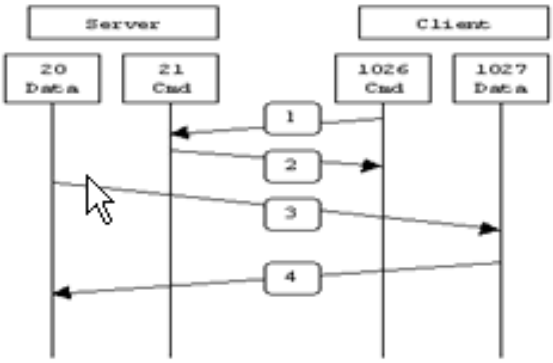
Inleiding

Dit document legt de stappen uit die voor gebruikers buiten uw netwerk vereist zijn om FTP- en TFTP-services in uw DMZ-netwerk te benaderen.

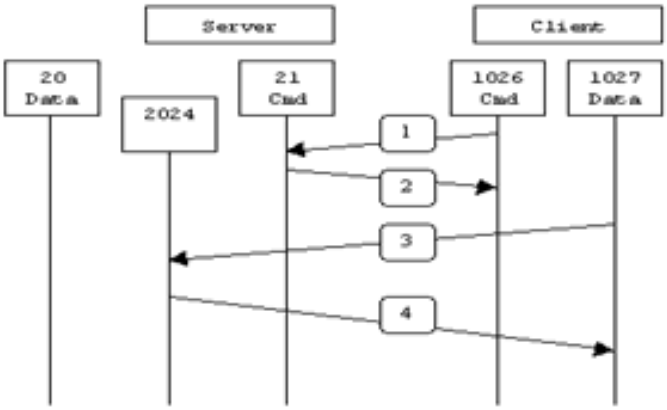
File Transfer Protocol (FTP)

Er zijn twee vormen van FTP:

- Actieve modus
- passieve modus



Active FTP



Passive FTP

Active FTP :
command : client >1023 -> server 21
data : client >1023 <- server 20

Passive FTP :
command : client >1023 -> server 21
data : client >1023 -> server >1023

In Actieve FTP-modus, sluit de client een willekeurige onbevoorrechte poort (N>1023) aan op de opdrachtpoort (21) van de FTP-server. Vervolgens luistert de client naar poort N+1 en stuurt de FTP-opdrachtpoort N+1 naar de FTP-server. De server sluit dan terug aan op de gespecificeerde gegevenspoorten van de client vanaf zijn lokale gegevenspoort, die poort 20 is.

In Passive FTP modus, opent de client beide verbindingen naar de server, wat het probleem oplost van een firewall die de inkomende verbinding van de gegevenspoort naar de client vanaf de server filtreert. Wanneer een FTP-verbinding wordt geopend, opent de client twee onbevoorrechte poorten lokaal (N>1023 en N+1). De eerste poort contacteert de server op port 21. Maar in plaats van dan een poortopdracht uit te geven en de server toe te staan om terug te verbinden met zijn gegevenspoort geeft de client de **PASV** opdracht uit. Het resultaat hiervan is dat de server dan een willekeurige onbevoorrechte poort opent (P>1023) en de Po-opdracht terugstuurt naar de client. De client start vervolgens de verbinding van poort N+1 naar poort P op de server om gegevens over te dragen. Zonder de configuratie van de **inspectie** op security applicatie, werkt FTP van binnenuit gebruikers naar buiten alleen in passieve modus. Ook wordt toegang geweigerd aan gebruikers buiten die naar uw FTP-server gaan.

Raadpleeg ASA 8.3 en hoger: Configuratievoorbeeld FTP/TFTP-services inschakelen voor meer informatie over identieke configuratie met behulp van ASDM met Cisco adaptieve security applicatie (ASA) met versie 8.3 en hoger.

Trial File Transfer Protocol (TFTP)

TFTP, zoals beschreven in RFC 1350, is een eenvoudig protocol om bestanden tussen een TFTP-server en client te lezen en schrijven. TFTP gebruikt UDP poort 69.

Voorwaarden

Vereisten

Zorg ervoor dat u aan deze vereisten voldoet voordat u deze configuratie probeert:

- Er is basiscommunicatie tussen de vereiste interfaces.
- U hebt een geconfigureerde FTP-server die zich in uw DMZ-netwerk bevindt.

Gebruikte componenten

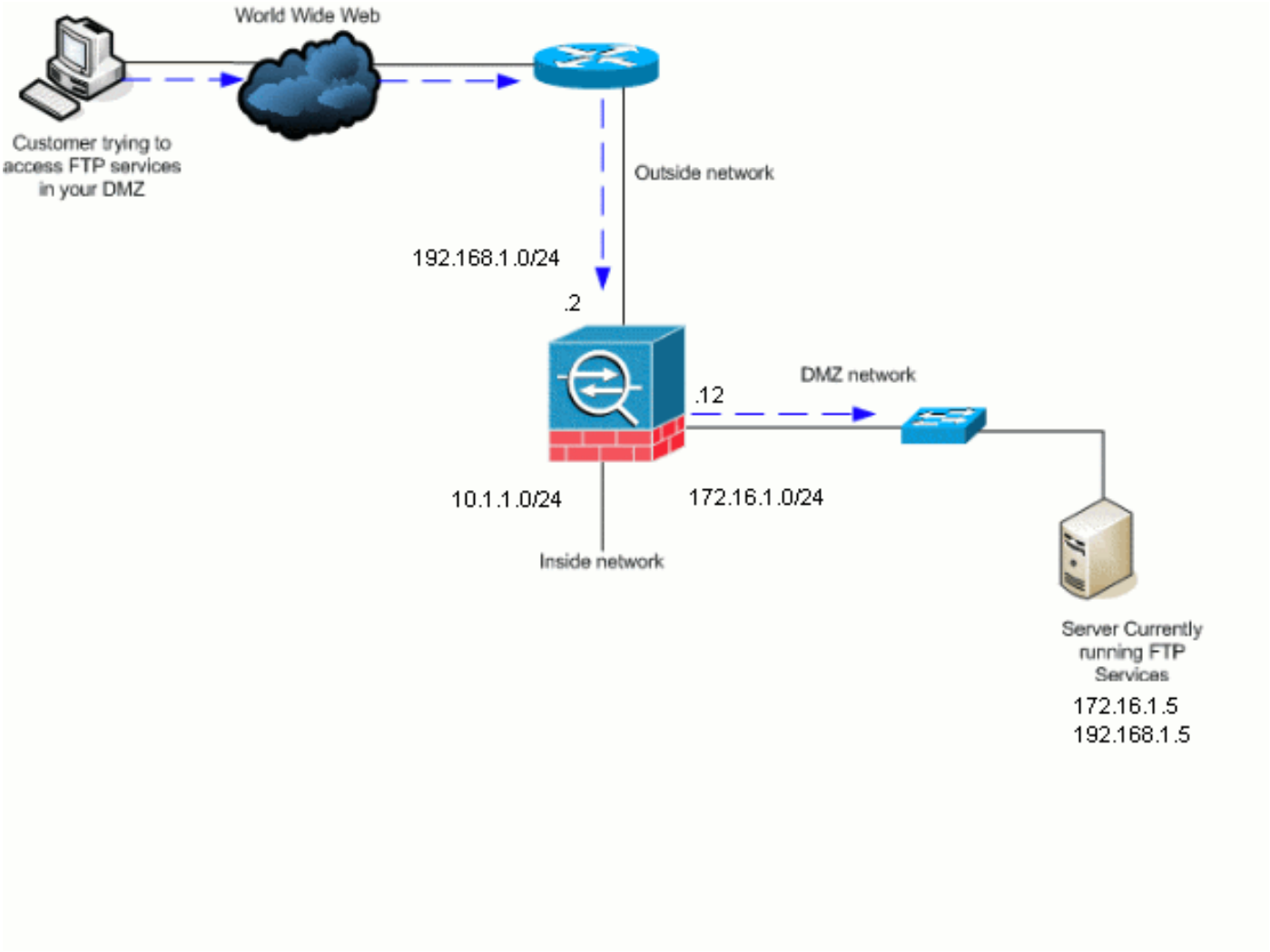
De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- ASA 5500 Series adaptieve security applicatie die ondersteuning biedt voor de 7.2(2) software-afbeelding
- Windows 2003 Server die FTP-services draait
- Windows 2003 Server die TFTP-services uitvoert
- Clientpc aan de buitenkant van het netwerk

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Netwerkdiagram

Het netwerk in dit document is als volgt opgebouwd:



OPMERKING: De IP-adresseringsschema's die in deze configuratie worden gebruikt, zijn niet wettelijk routeerbaar op het internet. Het zijn RFC 1918 adressen die in een labomgeving gebruikt zijn.

Verwante producten

Deze configuratie kan ook worden gebruikt met PIX security applicatie 7.x.

Conventies

Raadpleeg de Cisco Technical Tips Convention voor meer informatie over documentconventies.

Achtergrondinformatie

De security applicatie ondersteunt toepassingsinspectie via de functie Adaptieve security algoritme. Door de stateful Application inspection die door het Adaptieve Security Algorithm wordt gebruikt, volgt het Security Appliance elke verbinding die de firewall overslaat en garandeert dat deze geldig is. De firewall, door middel van stateful inspection, controleert ook de staat van de verbinding om informatie te compileren om in een staatstafel te plaatsen. Met het gebruik van de staatstabel in aanvulling op door de beheerder gedefinieerde regels, zijn de filterbeslissingen gebaseerd op context die wordt geconstrueerd door pakketten die eerder door de firewall zijn doorgegeven. De uitvoering van de toepassingsinspecties bestaat uit de volgende acties:

- Identificeer het verkeer.
- Inspecties op het verkeer toepassen.
- Activeert inspecties op een interface.

Geavanceerde protocolbehandeling

FTP

Sommige toepassingen vereisen speciale verwerking door de functie voor de inspectie van Cisco security applicatie. Deze toepassingen bevatten doorgaans IP-adresseringsinformatie in het gebruikerspakket of openen secundaire kanalen op dynamisch toegewezen poorten. De toepassingsinspectiefunctie werkt met Network Address Translation (NAT) om de locatie van ingesloten adresinformatie te bepalen.

Naast de identificatie van ingesloten adresseringsinformatie controleert de toepassingsinspectiefunctie sessies om de poortnummers voor secundaire kanalen te bepalen. Veel protocollen openen secundaire TCP- of UDP-poorten om de prestaties te verbeteren. De eerste sessie op een bekende haven wordt gebruikt om dynamisch toegewezen havennummers te onderhandelen. De toepassingsinspectiefunctie controleert deze sessies, identificeert de dynamische poortopdrachten en maakt gegevensuitwisseling op deze poorten mogelijk gedurende de specifieke sessies. Multimedia en FTP applicaties laten dit soort gedrag zien.

Het FTP-protocol vereist enige speciale behandeling vanwege het gebruik van twee poorten per FTP-sessie. Het FTP-protocol gebruikt twee poorten wanneer deze worden geactiveerd voor het verzenden van gegevens: een controlekanaal en een gegevenskanaal dat respectievelijk haven 21 en 20 gebruikt. De gebruiker, die de FTP-sessie over het controlekanaal initieert, doet alle gegevensverzoeken via dat kanaal. De FTP server start dan een verzoek om een poort van serverpoort 20 naar de computer van de gebruiker te openen. FTP gebruikt altijd poort 20 voor communicatie van gegevenskanalen. Als de FTP-inspectie niet op de security applicatie is ingeschakeld, wordt dit verzoek verworpen en worden de FTP-sessies geen gevraagde gegevens verzonden. Als FTP-inspectie is ingeschakeld op de security applicatie, controleert de security applicatie het controlekanaal en probeert deze een aanvraag te herkennen om het gegevenskanaal te openen. Het FTP-protocol stelt de poortspecificaties van het gegevenskanaal in het verkeer van het controlekanaal in elkaar, waarbij de security applicatie het controlekanaal moet inspecteren voor wijzigingen in de gegevenspoorten. Als de security applicatie een verzoek herkent, maakt deze tijdelijk een opening voor het data-kanaal verkeer dat geldig is voor het leven van de sessie. Op deze manier controleert de FTP-inspectiefunctie het controlekanaal, identificeert een data-poorts toewijzing en laat de informatie op de gegevenspoort voor de lengte van de sessie worden uitgewisseld.

De security applicatie inspecteert poort 21 verbindingen voor FTP-verkeer standaard door middel van de global-inspection class-map. De security applicatie erkent ook het verschil tussen een actieve en een passieve FTP-sessie. Als de FTP-sessies een passieve FTP-gegevensoverdracht ondersteunen, herkent de security applicatie, via de **inspectie ftp**-opdracht, het gegevenspoortverzoek van de gebruiker en opent een nieuwe gegevenspoort die groter is dan 1023.

De FTP-toepassingsinspectie inspecteert FTP-sessies en voert vier taken uit:

- voorbereidt een dynamische secundaire gegevensverbinding
- Traceert de opdracht-responsvolgorde van FTP

- genereert een controlespoor
- Vertaalt het ingesloten IP-adres met NAT

FTP-toepassingsinspectie bereidt secundaire kanalen voor voor FTP-gegevensoverdracht. De kanalen worden toegewezen in antwoord op een bestand uploaden, een bestand downloaden of een gebeurtenis met een directory-lijst, en zij moeten vooraf worden onderhandeld. De poort is onderhandeld via de opdrachten **PORT** of **PASV** (227).

TFTP

TFTP-inspectie is standaard ingeschakeld.

Het veiligheidsapparaat inspecteert TFTP-verkeer en creëert dynamisch verbindingen en vertalingen, indien nodig, om bestandsoverdracht tussen een TFTP-client en een TFTP-server mogelijk te maken. Met name de inspectiemachine inspecteert de TFTP-leesverzoeken (RRQ), schrijfverzoeken (WRQ) en foutmeldingen (FOUT).

Een dynamisch secundair kanaal en indien nodig een PAT-vertaling worden toegewezen op een ontvangst van een geldig RQ of WRQ. Dit secundaire kanaal wordt vervolgens door TFTP gebruikt voor bestandsoverdracht of foutmelding.

Alleen de TFTP-server kan het verkeer via het secundaire kanaal initiëren en er kan ten hoogste één onvolledig secundair kanaal bestaan tussen de TFTP-client en de server. Een foutmelding van de server sluit het secundaire kanaal.

TFTP-inspectie moet worden ingeschakeld indien statische PAT wordt gebruikt om TFTP-verkeer te herleiden.

Basis FTP-toepassingsinspectie configureren

Standaard omvat de configuratie een beleid dat overeenkomt met al het standaard toepassingsinspectieverkeer en past de inspectie op het verkeer op alle interfaces toe (een mondiaal beleid). Standaard toepassingsinspectieverkeer bevat verkeer naar de standaardpoorten voor elk protocol. Je kunt slechts één mondiaal beleid toepassen, dus als je het mondiale beleid wilt wijzigen, bijvoorbeeld om inspectie toe te passen op niet-standaard poorten, of om inspecties toe te voegen die standaard niet zijn ingeschakeld, moet je het standaardbeleid bewerken of uitschakelen en een nieuw beleid toepassen. Zie voor een lijst met alle standaardpoorten het beleid voor standaardinspectie.

1. Geef de **beleids-map global_policy** opdracht uit.
   ```
   ASAwAIP-CLI(config)#policy-map global_policy
   ```

2. Geef de **class inspection_default** opdracht uit.
   ```
   ASAwAIP-CLI(config-pmap)#class inspection_default
   ```

3. Geef de **FTP-**opdracht af.
   ```
   ASAwAIP-CLI(config-pmap-c)#inspect FTP
   ```

   Er is een optie om de **strikte** opdracht **FTP** te gebruiken. Deze opdracht verhoogt de beveiliging van beschermde netwerken door te voorkomen dat een webbrowser ingesloten opdrachten in FTP-aanvragen verzenden.Nadat u de *strikte* optie op een interface hebt

ingeschakeld, dwingt FTP-inspectie dit gedrag af:Een FTP-opdracht moet worden erkend voordat de security applicatie een nieuwe opdracht geeft.De security applicatie laat een verbinding vallen die ingesloten opdrachten verstuurt.De opdrachten **227** en **PORT** worden gecontroleerd om er zeker van te zijn dat ze niet in een foutmelding verschijnen.**Waarschuwing:** het gebruik van de **strikte** optie kan de storing van FTP clients veroorzaken die niet volledig compatibel zijn met FTP RFC's. Raadpleeg De strikte optie gebruiken voor meer informatie over het gebruik van de *strikte **optie.***

Configuratievoorbeeld

Apparaatnaam 1

```
ASA-AIP-CLI(config)#show running-config

 ASA Version 7.2(2)
!
hostname ASA-AIP-CLI
domain-name corp.com
enable password WwXYvtKrnjXqGbu1 encrypted
names
!
interface Ethernet0/0
 nameif Outside
 security-level 0
 ip address 192.168.1.2 255.255.255.0
!
interface Ethernet0/1
 nameif Inside
 security-level 100
ip address 10.1.1.1 255.255.255.0
!
interface Ethernet0/2
 nameif DMZ
  security-level 50
  ip address 172.16.1.12 255.255.255.0
!
interface Ethernet0/3
 no nameif
 no security-level
 no ip address
!
interface Management0/0
  no nameif
 no security-level
 no ip address
!
!--- Output is suppressed. !--- Permit inbound FTP
control traffic. access-list 100 extended permit tcp any
host 192.168.1.5 eq ftp
!--- Permit inbound FTP data traffic. access-list 100
extended permit tcp any host 192.168.1.5 eq ftp-data
!
!--- Command to redirect the FTP traffic received on IP
192.168.1.5 !--- to IP 172.16.1.5. static (DMZ,outside)
192.168.1.5 172.16.1.5 netmask 255.255.255.255
access-group 100 in interface outside
class-map inspection_default
 match default-inspection-traffic
!
```

```
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum 512

policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
!
!--- This command tells the device to !--- use the
"global_policy" policy-map on all interfaces. service-
policy global_policy global
prompt hostname context
Cryptochecksum:4b2f54134e685d11b274ee159e5ed009
: end
ASA-AIP-CLI(config)#
```

Configuratie FTP-protocolinspectie op niet-standaard TCP-poort

U kunt de FTP Protocol-inspectie voor niet-standaard TCP-poorten configureren met deze configuratie-lijnen (XXXX vervangen door het nieuwe poortnummer):

```
access-list ftp-list extended permit tcp any any eq XXXX
!
class-map ftp-class
  match access-list ftp-list
!
policy-map global_policy
  class ftp-class
   inspect ftp
```

Basis TFTP-toepassingsinspectie configureren

Standaard omvat de configuratie een beleid dat overeenkomt met al het standaard toepassingsinspectieverkeer en past de inspectie op het verkeer op alle interfaces toe (een mondiaal beleid). Standaard toepassingsinspectieverkeer bevat verkeer naar de standaardpoorten voor elk protocol. Je kunt maar één mondiaal beleid toepassen. Dus als je het mondiale beleid wilt wijzigen, bijvoorbeeld, om inspectie toe te passen op niet standaardpoorten, of om inspecties toe te voegen die standaard niet ingeschakeld zijn, moet je het standaardbeleid bewerken of uitschakelen en een nieuw beleid toepassen. Zie voor een lijst met alle standaardpoorten het beleid voor standaardinspectie.

1. Geef de **beleids-map global_policy** opdracht uit.

```
ASAwAIP-CLI(config)#policy-map global_policy
```

2. Geef de **class inspection_default** opdracht uit.
```
ASAwAIP-CLI(config-pmap)#class inspection_default
```

3. Geef de opdracht **TFTP** uit.
```
ASAwAIP-CLI(config-pmap-c)#inspect TFTP
```

Configuratievoorbeeld

Apparaatnaam 1

```
ASA-AIP-CLI(config)#show running-config

 ASA Version 7.2(2)
!
hostname ASA-AIP-CLI
domain-name corp.com
enable password WwXYvtKrnjXqGbu1 encrypted
names
!
interface Ethernet0/0
 nameif Outside
 security-level 0
 ip address 192.168.1.2 255.255.255.0
!
interface Ethernet0/1
 nameif Inside
 security-level 100
ip address 10.1.1.1 255.255.255.0
!
interface Ethernet0/2
 nameif DMZ
  security-level 50
  ip address 172.16.1.12 255.255.255.0
!
interface Ethernet0/3
 no nameif
 no security-level
 no ip address
!
interface Management0/0
  no nameif
 no security-level
 no ip address
!
!--- Output is suppressed. !--- Permit inbound TFTP
traffic. access-list 100 extended permit udp any host
192.168.1.5 eq tftp
!
!--- Command to redirect the TFTP traffic received on IP
192.168.1.5 !--- to IP 172.16.1.5. static (DMZ,outside)
192.168.1.5 172.16.1.5 netmask 255.255.255.255
access-group 100 in interface outside
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
```

```
 parameters
  message-length maximum 512

policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
!
!--- This command tells the device to !--- use the
"global_policy" policy-map on all interfaces. service-
policy global_policy global
prompt hostname context
Cryptochecksum:4b2f54134e685d11b274ee159e5ed009
: end
ASA-AIP-CLI(config)#
```

Verifiëren

Om ervoor te zorgen dat de configuratie succesvol is uitgevoerd, gebruik de opdracht **showservice-beleid** en beperkt de output tot alleen de FTP-inspectie, met behulp van de **show service-policy inspectie ftp** opdracht.

```
ASAwAIP-CLI# show service-policy inspect ftp

Global policy:
  Service-policy: global_policy
    Class-map: inspection_default
      Inspect: ftp, packet 0, drop 0, reset-drop 0
ASAwAIP-CLI#
```

Problemen oplossen

Probleem: Syntax in Configuration not Work and class-map inspection Error wordt ontvangen

De syntaxis die in het configuratiegedeelte wordt weergegeven, werkt niet en u ontvangt een fout als deze:

```
ERROR: % class-map inspection_default not configured
```

Oplossing

Deze configuratie is afhankelijk van de standaardinstellingen die worden uitgevoerd in de

configuratie. Als zij niet in de configuratie zijn, kunt u deze met deze opdrachten herhalen:

1. **class-map inspectie_defaultovereenkomende met standaardinspectie-verkeer**
2. **beleidsplan-kaarttype inspectie dns vooraf ingestelde_dns_map parametersberichtlengte maximaal 512**
3. **beleidsmatig 'global_policy'class inspection_defaultinspecteer dns vooraf ingestelde_dns_mapinspectie van ftp - inspectie h323 h225h323 ras controlereninspectereninspecteren van rtspinspectie esmtpsqlnet inspectereninspectie van magiezonnecomputer controlerenxdmcp inspectereninspecteren van het schipnetbios inspectereninspectie van tftp**
4. **global_policy voor diensten**

Waarschuwing: Als de standaardinspecties eerder zijn verwijderd om een ander probleem op te lossen, kan dat probleem terugkeren als de standaardinspecties opnieuw worden ingeschakeld. U of uw beheerder moet weten of de standaardinspecties eerder zijn verwijderd als een stap voor het oplossen van problemen.

Kan FTPS (FTP over SSL) over ASA niet starten

FTP met TLS/SSL (SFTP/FTPS) wordt niet ondersteund door de security applicatie. De FTP-verbinding is versleuteld, zodat de firewall het pakket niet kan decrypteren. Raadpleeg PIX/ASA: Security applicatie FAQ voor meer informatie.

Gerelateerde informatie

- ASA 5500 Series adaptieve security applicaties
- Opdracht voor Cisco security applicatie
- PIX 500 Series security applicatie
- Cisco Security Advisories en kennisgevingen
- Technische ondersteuning en documentatie – Cisco Systems