SSL VPN-client (SVC) op ASA met ASDM Configuration Voorbeeld

Inhoud

Inleiding

Met Secure Socket Layer (SSL) Virtual Private Network (VPN)-technologie kunt u veilig vanaf elke locatie verbinding maken met een intern bedrijfsnetwerk via een van deze methoden:

- Clientless SSL VPN (WebVPN)—Biedt een externe client waarvoor een SSL-enabled webbrowser nodig is voor toegang tot HTTP- of HTTPS-webservers op een lokaal netwerk

van het bedrijf (LAN). Daarnaast biedt clientloze SSL VPN toegang voor het bladeren door Windows-bestanden via het CIFS-protocol (Common Internet File System). Outlook Web Access (OWA) is een voorbeeld van HTTP-toegang.

Raadpleeg Clientless SSL VPN (WebVPN) bij ASA Configuration Voorbeeld om meer te weten te komen over Clientless SSL VPN.

- Thin-client SSL VPN (poortdoorsturen)—Biedt een externe client die een kleine op Java gebaseerde applet downloadt en beveiligde toegang biedt voor TCP-toepassingen (Transmission Control Protocol) die statische poortnummers gebruiken. Post Office Protocol (POP3), Simple Mail Transfer Protocol (SMTP), Internet Message Access Protocol (IMAP), Secure Shell (SSH) en Telnet zijn voorbeelden van beveiligde toegang. Omdat bestanden op de lokale machine worden gewijzigd, moeten gebruikers lokale administratieve rechten hebben om deze methode te gebruiken. Deze methode van SSL VPN werkt niet met toepassingen die dynamische poorttoewijzingen gebruiken, zoals sommige FTP-toepassingen (File Transfer Protocol).

  Raadpleeg Thin-Client SSL VPN (WebVPN) op ASA met ASDM Configuration Voorbeeld om meer te weten te komen over Thin-client SSL VPN.

  Opmerking: User Datagram Protocol (UDP) wordt niet ondersteund.

- SSL VPN Client (Tunnel Mode)—Downloads een kleine client naar het externe werkstation en biedt volledige beveiligde toegang tot resources op een intern bedrijfsnetwerk. U kunt de SSL VPN-client (SVC) permanent downloaden naar een extern werkstation of u kunt de client verwijderen zodra de beveiligde sessie is gesloten.

Dit document beschrijft hoe u de SVC kunt configureren op een adaptieve security applicatie (ASA) met behulp van Adaptieve security apparaatbeheer (ASDM). De opdrachtregels die uit deze configuratie voortvloeien, worden vermeld in de sectie Resultaten.

Voorwaarden

Vereisten

Zorg ervoor dat u aan de volgende voorwaarden voldoet voordat u deze configuratie uitvoert:

- SVC start ondersteuning van Cisco adaptieve security applicatie versie 7.1 en hoger
- Lokale administratieve rechten op alle externe werkstations
- Java- en ActiveX-besturingselementen op het externe werkstation
- Port 443 is niet ergens geblokkeerd langs het verbindingspad

Gebruikte componenten

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

- Software voor Cisco adaptieve security applicatie versie 7.2(1)
- Cisco Adaptieve Security Device Manager 5.2(1)
- Cisco adaptieve security applicatie 5510 Series
- Microsoft Windows XP Professional SP 2

De informatie in dit document is ontwikkeld in een laboratoriumomgeving. Alle apparaten die in dit document zijn gebruikt, zijn teruggezet op de standaardconfiguratie. Als uw netwerk live is, zorg er dan voor dat u de potentiële impact van een opdracht begrijpt. Alle IP-adressen die in deze configuratie worden gebruikt, zijn geselecteerd uit RFC 1918-adressen in een laboratoriumomgeving; deze IP-adressen zijn niet routeerbaar op internet en zijn alleen voor testdoeleinden.

Netwerkdiagram

Dit document gebruikt de netwerkconfiguratie die in deze sectie wordt beschreven.

Een externe gebruiker maakt verbinding met het IP-adres van de ASA met een SSL-compatibele webbrowser. Na succesvolle verificatie wordt de SVC gedownload naar de clientcomputer en kan de gebruiker een versleutelde beveiligde sessie gebruiken voor volledige toegang tot alle toegestane bronnen op het bedrijfsnetwerk.

Taken voor preconfiguratie

Voltooi voordat u begint de volgende taken:

- Verwijs naar Toestaan van HTTPS-toegang voor ASDM zodat de ASA door de ASDM kan worden geconfigureerd.

  Om toegang te krijgen tot de ASDM-toepassing, vanaf uw beheerstation, gebruikt u een SSL-enabled webbrowser en voert u het IP-adres van het ASA-apparaat in. Bijvoorbeeld: https://inside_ip_address, waar inside_ip_address het adres van de ASA is. Nadat ASDM is geladen, kunt u de configuratie van de SVC starten.

- Download het SSL VPN-clientpakket (slclient-win*.pkg) van de website Cisco Software Download (alleen geregistreerde klanten) naar de lokale vaste schijf van het beheerstation waar u toegang tot de ASDM-toepassing hebt.

WebVPN en ASDM kunnen niet op dezelfde ASA interface worden ingeschakeld tenzij u de poortnummers wijzigt. Als u wilt dat de twee technologieën dezelfde poort (poort 443) op hetzelfde apparaat gebruiken, kunt u ASDM inschakelen op de binnenkant interface en WebVPN inschakelen op de buiteninterface.

Conventies

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

De SSL VPN-client op een ASA configureren

Voltooi de volgende stappen om de SSL VPN-client op een ASA te configureren:

1. Web VPN-toegang inschakelen op de ASA
2. De SSL VPN-client op de ASA installeren en inschakelen
3. SVC-installatie op clients inschakelen
4. Rekey-parameters inschakelen

Stap 1. Web VPN-toegang inschakelen op de ASA

Voltooi de volgende stappen om WebVPN-toegang via de ASA in te schakelen:

1. Klik binnen de ASDM-toepassing op Configuration en vervolgens op VPN.
2. Breid WebVPN uit en kies WebVPN Access.
3. Selecteer de interface waarvoor u WebVPN wilt inschakelen en klik op Inschakelen.

Stap 2. De SSL VPN-client op de ASA installeren en inschakelen

Voltooi de volgende stappen om de SSL VPN-client op de ASA te installeren en in te schakelen:

1. Klik op Configuration en vervolgens op VPN.
2. Vouw WebVPN uit in het navigatiedeelvenster en kies SSL VPN-client.
3. Klik op Add (Toevoegen).

   Het dialoogvenster SSL VPN-clientafbeelding toevoegen verschijnt.
4. Klik op de knop Upload.

   Het dialoogvenster Afbeelding uploaden verschijnt.
5. Klik op de knop Local Files om een bestand op uw lokale computer te vinden of klik op de knop Bladeren Flash om een bestand op het flash-bestandssysteem te vinden.
6. Zoek het te uploaden clientbeeldbestand en klik op OK.
7. Klik op Upload File en klik vervolgens op Close.
8. Zodra het cliëntbeeld om wordt geladen te flitsen, controleer het de controlevakje van de Enable SSL VPN Cliënt, en klik dan van toepassing zijn.

   Opmerking: Als u een foutbericht ontvangt, controleert u of WebVPN-toegang is ingeschakeld. Vouw WebVPN uit in het navigatiedeelvenster en kies WebVPN Access.

Selecteer de interface waarvoor u toegang wilt configureren en klik op Inschakelen.

9. Klik op Opslaan en klik vervolgens op Ja om de wijzigingen te aanvaarden.

Stap 3. SVC-installatie op clients inschakelen

Voltooi de volgende stappen om SVC-installatie op clients in te schakelen:

1. Vouw in het navigatiedeelvenster IP-adresbeheer uit en kies IP-pools.
2. Klik op Add en voer waarden in de velden Naam, IP-adres starten, IP-adres beëindigen en Subnetmasker in. De IP-adressen die u invoert voor de velden Start IP-adres en Laatste IP-adres moeten afkomstig zijn van subnetten in uw interne netwerk.
3. Klik op OK en klik vervolgens op Toepassen.
4. Klik op Opslaan en klik vervolgens op Ja om de wijzigingen te aanvaarden.
5. Vouw in het navigatiedeelvenster IP-adresbeheer uit en kies Toewijzing.
6. Schakel het aanvinkvakje Interne adrespools gebruiken in en schakel vervolgens de selectievakjes Verificatieserver gebruiken en DHCP gebruiken uit.
7. Klik op Apply (Toepassen).
8. Klik op Opslaan en klik vervolgens op Ja om de wijzigingen te aanvaarden.
9. In het navigatiedeelvenster vouwt u Algemeen uit en kiest u Tunnelgroep.
10. Selecteer de tunnelgroep die u wilt beheren en klik op Bewerken.
11. Klik op het tabblad Toewijzing clientadres en selecteer de nieuwe IP-adresgroep in de lijst Beschikbare pools.
12. Klik op Add en vervolgens op OK.
13. Klik in het ASDM-toepassingsvenster op Toepassen.
14. Klik op Opslaan en klik vervolgens op Ja om de wijzigingen te aanvaarden.

Stap 4. Rekey-parameter inschakelen

Zo schakelt u rekey-parameters in:

1. Vouw in het navigatiedeelvenster Algemeen uit en kies Groepsbeleid.
2. Selecteer het beleid dat u op deze groep van clients wilt toepassen en klik op Bewerken.
3. Op het tabblad Algemeen verwijdert u het aanvinkvakje Tunneling Protocollen en schakelt u het aanvinkvakje WebVPN in.

4. Klik op het tabblad WebVPN, klik op het tabblad SSL VPN-client en kies deze opties:

    a. Voor de optie SSL VPN-client gebruiken, deselecteert u het aanvinkvakje Inherit en klikt u op het keuzerondje Optioneel.

    Met deze keuze kan de externe client kiezen of hij de SVC wil downloaden of niet. De Altijd keuze zorgt ervoor dat de SVC wordt gedownload naar het externe werkstation tijdens elke SSL VPN verbinding.

    b. Voor de optie Installateur op clientsysteem behouden, deselecteert u het aanvinkvakje Inherit en klikt u op de knop Ja.

    Hierdoor kan de SVC-software op de clientmachine blijven; de ASA hoeft de SVC-software daarom niet telkens wanneer een verbinding wordt gemaakt naar de client te downloaden. Deze optie is een goede keuze voor externe gebruikers die vaak toegang hebben tot het bedrijfsnetwerk.

    c. Voor de optie Heronderhandelingsinterval uitschakelt u het vakje Inherit uit, het selectievakje Onbeperkt en voert u het aantal minuten in totdat u opnieuw inschakelt.

    De beveiliging wordt verbeterd door limieten in te stellen aan de tijdsduur dat een sleutel geldig is.

    d. Voor de optie Heronderhandelingsmethode deselecteert u het aanvinkvakje Inherit en klikt u op het keuzerondje SSL. Heronderhandeling kan de huidige SSL-tunnel of een nieuwe tunnel gebruiken die uitdrukkelijk voor heronderhandeling is gemaakt.

    Uw SSL VPN-clientkenmerken moeten worden geconfigureerd zoals in deze afbeelding:

5. Klik op OK en klik vervolgens op Toepassen.

6. Klik op Opslaan en klik vervolgens op Ja om de wijzigingen te aanvaarden.

Resultaten

Met de ASDM worden deze configuraties in de opdrachtregel gemaakt:

ciscoasa
<#root> ciscoasa(config)# **show run** ASA Version 7.2(1) ! hostname ciscoasa domain-name cisco.com enable password 9jNfZuG3TC5tCVH0 encrypted

```
names
dns-guard
!
interface Ethernet0/0
 nameif outside
 security-level 0
 ip address 172.22.1.160 255.255.255.0
!
interface Ethernet0/1
 nameif inside
 security-level 100
 ip address 10.2.2.1 255.255.255.0
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
dns server-group DefaultDNS
 domain-name cisco.com
no pager
logging enable
logging asdm informational
mtu outside 1500
mtu inside 1500
mtu DMZ1 1500
mtu Mgt 1500
ip local pool CorporateNet 10.2.2.50-10.2.2.60 mask 255.255.255.0
icmp permit any outside
asdm image disk0:/asdm521.bin
no asdm history enable
arp timeout 14400
global (outside) 1 interface
nat (inside) 1 0 0
route outside 0.0.0.0 0.0.0.0 172.22.1.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout uauth 0:05:00 absolute
!

!--- Group Policy Statements

group-policy GroupPolicy1 internal
group-policy GroupPolicy1 attributes
 vpn-tunnel-protocol IPSec l2tp-ipsec webvpn

!--- Enable the SVC for WebVPN

 webvpn
  svc enable
  svc keep-installer installed
  svc rekey time 30
  svc rekey method ssl
!
username cisco password 53QNetqK.Kqqfshe encrypted privilege 15
!
http server enable
http 10.2.2.0 255.255.255.0 inside
!
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart

!--- Tunnel Group and Group Policy using the defaults here
```

```
tunnel-group DefaultWEBVPNGroup general-attributes
 address-pool CorporateNet
 default-group-policy GroupPolicy1
!
no vpn-addr-assign aaa
no vpn-addr-assign dhcp
!
telnet timeout 5
ssh 172.22.1.0 255.255.255.0 outside
ssh timeout 5
console timeout 0
!
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 rsh
  inspect rtsp
  inspect esmtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
!
service-policy global_policy global

!--- Enable webvpn and the select the SVC client

webvpn
 enable outside
 svc image disk0:/sslclient-win-1.1.1.164.pkg 1
 svc enable

!--- Provide list for access to resources

 url-list ServerList "E-Commerce Server1" http://10.2.2.2 1
 url-list ServerList "BrowseServer" cifs://10.2.2.2 2
 tunnel-group-list enable

prompt hostname context
Cryptochecksum:80a1890a95580dca11e3aee200173f5f
: end
```

Pas uw configuratie aan

De procedures die in Configure de SSL VPN-client op een ASA worden beschreven, gebruiken de ASA-standaardnamen voor groepsbeleid (GroupPolicy1) en tunnelgroep (DefaultWebVPNGGroup) zoals in deze afbeelding:

Deze procedure beschrijft hoe u uw eigen maatwerkgroepbeleid en tunnelgroepen kunt maken en deze kunt koppelen in overeenstemming met het beveiligingsbeleid van uw organisatie.

Voltooi de volgende stappen om de configuratie aan te passen:

1. Een aangepast groepsbeleid maken
2. Een aangepaste tunnelgroep maken
3. Maak een gebruiker en voeg die gebruiker toe aan uw beleid voor aangepaste groepen

Stap 1. Een aangepast groepsbeleid maken

Voltooi de volgende stappen om een aangepast groepsbeleid te maken:

1. Klik op Configuration en vervolgens op VPN.
2. Algemeen uitvouwen en groepsbeleid kiezen.
3. Klik op Add en kies Interne Groepsbeleid.
4. Voer in het veld Naam een naam in voor uw groepsbeleid.

   In dit voorbeeld is de naam van het groepsbeleid gewijzigd in SalesGroupPolicy.
5. Onder het tabblad Algemeen schakelt u het aanvinkvakje Tunneling Protocollen overnemen uit en schakelt u het aanvinkvakje WebVPN in.
6. Klik op het tabblad WebVPN en klik vervolgens op het tabblad SSL VPN Client.

   In dit dialoogvenster kunt u ook keuzes maken voor het gedrag van de SSL VPN-client.
7. Klik op OK en klik vervolgens op Toepassen.
8. Klik op Opslaan en klik vervolgens op Ja om de wijzigingen te aanvaarden.

Stap 2. Een aangepaste tunnelgroep maken

Voltooi de volgende stappen om een aangepaste tunnelgroep te maken:

1. Klik op de knop Configuration en klik vervolgens op VPN.
2. Algemeen uitvouwen en Tunnelgroep kiezen.
3. Klik op Add en kies Web VPN Access.
4. Typ in het veld Naam een naam voor de tunnelgroep.

In dit voorbeeld is de naam van de tunnelgroep gewijzigd in SalesForceGroup.

5. Klik op de vervolgkeuzepijl Groepsbeleid en kies uw nieuwe groepsbeleid.

   Uw groepsbeleid en tunnelgroep zijn nu verbonden.

6. Klik op het tabblad Toewijzing clientadres en voer informatie over DHCP-server in of selecteer een lokaal gemaakte IP-pool.
7. Klik op OK en klik vervolgens op Toepassen.
8. Klik op Opslaan en klik vervolgens op Ja om de wijzigingen te aanvaarden.

Stap 3. Maak een gebruiker en voeg die gebruiker toe aan uw beleid voor aangepaste groepen

Voltooi de volgende stappen om een gebruiker te maken en die gebruiker toe te voegen aan uw aangepaste groepsbeleid:

1. Klik op Configuration en vervolgens op VPN.
2. Algemeen uitvouwen en Gebruikers kiezen.
3. Klik op Add en voer de gebruikersnaam en het wachtwoord in.
4. Klik op het tabblad VPN-beleid. Zorg ervoor dat uw nieuwe groepsbeleid wordt weergegeven in het veld Groepsbeleid.

   Deze gebruiker erft alle kenmerken van het nieuwe groepsbeleid.

5. Klik op OK en klik vervolgens op Toepassen.
6. Klik op Opslaan en klik vervolgens op Ja om de wijzigingen te aanvaarden.

Verifiëren

Gebruik deze sectie om te controleren of uw configuratie goed werkt.

Verificatie

Verificatie voor SSL VPN-clients wordt uitgevoerd met een van deze methoden:

- Cisco Secure ACS-server (RADIUS)
- NT-domein
- Active Directory
- Eenmalige wachtwoorden

- Digitale certificaten
- Smartcards
- Lokale AAA-verificatie

In deze documentatie wordt een lokale account gebruikt die op het ASA-apparaat is gemaakt.

Opmerking: als een adaptieve security applicatie meerdere trustpoints heeft die dezelfde CA delen, kan slechts één van deze trustpoints die de CA delen worden gebruikt om gebruikerscertificaten te valideren.

Configuratie

Als u met de ASA verbinding wilt maken met een externe client, voert u https://ASA_outside_address in het adresveld van een SSL-compatibele webbrowser. ASA_external_address is het buitenste IP-adres van uw ASA. Als de configuratie is geslaagd, wordt het venster voor de client voor Cisco Systems SSL VPN weergegeven.

Opmerking: het venster voor de client voor Cisco Systems SSL VPN verschijnt alleen nadat u het certificaat van de ASA hebt aanvaard en nadat de SSL VPN-client is gedownload naar het externe station. Als het venster niet wordt weergegeven, zorg er dan voor dat het niet wordt geminimaliseerd.

Opdrachten

Verscheidene show bevelen worden geassocieerd met WebVPN. U kunt deze opdrachten uitvoeren via de opdrachtregelinterface (CLI) om statistieken en andere informatie te tonen. Raadpleeg Web VPN-configuraties verifiëren voor uitgebreide informatie over de show-opdrachten.

Opmerking: De Output Interpreter Tool (alleen geregistreerde klanten) (OIT) ondersteunt bepaalde show opdrachten. Gebruik de OIT om een analyse te bekijken van de output van de opdracht show.

Problemen oplossen

Deze sectie bevat informatie om uw configuratie te troubleshooten.

SVC-fout

Probleem

Mogelijk ontvangt u deze foutmelding tijdens de verificatie:

```
"The SSl VPN connection to the remote peer was disrupted
and could not be automatically re-estabilished. A new connection requires
```

```
re-authentication and must be restarted manually. Close all sensitive networked
applications."
```

Oplossing

Als er een firewallservice op uw pc wordt uitgevoerd, kan deze de verificatie onderbreken. Stop de service en sluit de client opnieuw aan.

Heeft de SVC een beveiligde sessie met de ASA ingesteld?

Om er zeker van te zijn dat de SSL VPN-client een beveiligde sessie met de ASA heeft ingesteld:

1. Klik op Bewaking.
2. Breid VPN-statistieken uit en kies Sessies.
3. Kies SSL VPN-client in het vervolgkeuzemenu Filter op VPN en klik op de knop Filter.

   Uw configuratie moet in de sessielijst verschijnen.

Worden beveiligde sessies succesvol aangemaakt en beëindigd?

U kunt de real-time logbestanden bekijken om er zeker van te zijn dat sessies met succes worden gestart en beëindigd. U kunt sessielogboeken als volgt weergeven:

1. Klik op Bewaking en vervolgens op Vastlegging.
2. Kies de Real-time Log Viewer of Log Buffer, en klik vervolgens op Weergeven.

   Opmerking: Alleen sessies van een specifiek adres weergeven, filter op adres.

Controleer de IP-pool in Web VPN Profile

```
%ASA-3-722020: Group group User user-name IP IP_address  No address
available for SVC connection
```

Er zijn geen adressen beschikbaar om toe te wijzen aan de SVC-verbinding. Wijs daarom het IP-pooladres toe in het profiel.

Als u het nieuwe verbindingsprofiel maakt, moet u een alias of groep-url configureren om toegang te krijgen tot dit verbindingsprofiel. Als dit niet het geval is, zullen alle SSL-pogingen het standaard WebVPN-verbindingsprofiel raken dat geen IP-pool aan het profiel was gekoppeld. Stel deze optie in om het standaardverbindingsprofiel te gebruiken en er een IP-pool op te plaatsen.

Tips

- Zorg ervoor dat routing goed werkt met de IP-adrespool die u aan uw externe clients toewijst. Deze IP-adresgroep moet afkomstig zijn van een subnetverbinding op uw LAN. U kunt ook een DHCP-server of verificatieserver gebruiken om IP-adressen toe te wijzen.
- De ASA maakt een standaardtunnelgroep (DefaultWebVPNGGroup) en een standaardgroepsbeleid (GroupPolicy1). Als u nieuwe groepen en beleid maakt, moet u ervoor zorgen dat u waarden toepast in overeenstemming met het beveiligingsbeleid van uw netwerk.
- Als u het doorbladeren van Windows-bestanden via CIFS wilt inschakelen, voert u een WINS-server (NBNS) in onder Configuration > VPN > WebVPN > Servers en URL's. Deze technologie maakt gebruik van de CIFS-selectie.

Opdrachten

Verscheidene debug bevelen worden geassocieerd met WebVPN. Zie Opdrachten voor gedetailleerde informatie over deze opdrachten gebruiken met WebVPN Debug Commands.

Opmerking: het gebruik van debug-opdrachten kan een nadelige invloed hebben op uw Cisco-apparaat. Raadpleeg Important Information on Debug Commands (Belangrijke informatie over opdrachten met debug) voordat u debug-opdrachten opgeeft.

Gerelateerde informatie

- Clientloze SSL VPN (WebVPN) op ASA Configuration Voorbeeld
- Thin-client SSL VPN (WebVPN) op ASA met ASDM Configuration Voorbeeld
- ASA met WebVPN en Single Sign-on met ASDM en NTLMv1 Configuration Voorbeeld
- Adaptieve security applicaties van Cisco ASA 5500 Series
- Technische ondersteuning en documentatie – Cisco Systems

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.