Exemplo de Configuração de Cliente VPN SSL (SVC) no ASA com o ASDM

Índice

Introdução

A tecnologia de Rede Privada Virtual (VPN) com Secure Socket Layer (SSL) permite que você se conecte com segurança de qualquer lugar a uma rede corporativa interna usando um dos seguintes métodos:

- **Sem clientes SSL VPN (WebVPN)** — Fornece um cliente remoto que exija um navegador da Web SSL-permitido alcançar servidores de Web HTTP ou HTTPS em uma rede de área local (LAN) corporativa. Além, os sem clientes SSL VPN fornecem o acesso para o arquivo de Windows que consulta com o protocolo do Common Internet File System (CIFS). O acesso à Web da probabilidade (OWA) é um acesso do exemplo de HTTP.Refira os sem clientes SSL VPN (WebVPN) no exemplo de configuração ASA a fim aprender mais sobre os sem clientes SSL VPN.
- **O thin client SSL VPN (transmissão da porta)** — fornece um cliente remoto que transfira um applet com base em Java pequeno e permite o acesso seguro para os aplicativos do Transmission Control Protocol (TCP) que usam números de porta estática. O protocolo Post Office Protocol (POP3), o Simple Mail Transfer Protocol (SMTP), o Internet Message Access Protocol (IMAP), o Shell Seguro (ssh), e o telnet são exemplos do acesso seguro. Porque os arquivos na máquina local mudam, os usuários devem ter privilégios administrativos locais usar este método. Este método de SSL VPN não trabalha com aplicativos que usam atribuições de porta dinâmica, tais como alguns aplicativos do File Transfer Protocol (FTP).Refira o thin client SSL VPN (WebVPN) no ASA com exemplo da configuração ASDM a fim aprender mais sobre o thin client SSL VPN.**Note**: O User Datagram Protocol (UDP) não é apoiado.
- **Cliente VPN SSL (modo de túnel)** — Transfere um cliente pequeno à estação de trabalho remota e permite o acesso seguro completo aos recursos em uma rede corporativa interna. Você pode transferir o cliente VPN SSL (SVC) a uma estação de trabalho remota permanentemente, ou você pode remover o cliente uma vez que a sessão segura é fechada.

Este documento descreve como configurar o SVC em uma ferramenta de segurança adaptável (ASA) que usa o Security Device Manager adaptável (ASDM). As linhas de comando que resultam desta configuração são alistadas na seção dos resultados.

Pré-requisitos

Requisitos

Antes de você tentar esta configuração, verifique se estes requisitos são atendidos:

- Apoio dos começos SVC da versão de software adaptável 7.1 da ferramenta de segurança de Cisco e mais atrasado
- Privilégios administrativos locais em todas as estações de trabalho remota
- Javas e controles activex na estação de trabalho remota
- A porta 443 não é obstruída em qualquer lugar ao longo do caminho de conexão

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Versão de software adaptável da ferramenta de segurança de Cisco 7.2(1)
- Cisco Adaptive Security Device Manager 5.2(1)
- 5510 Series adaptável da ferramenta de segurança de Cisco
- Microsoft Windows XP SP2 profissional

A informação neste documento foi desenvolvida em um ambiente de laboratório. Todos os

dispositivos usados neste documento começado foram restaurados a sua configuração padrão. Se sua rede está viva, certifique-se de você compreender o impacto potencial do comando any. Todos os endereços IP de Um ou Mais Servidores Cisco ICM NT usados nesta configuração foram selecionados dos endereços do RFC 1918 em um ambiente de laboratório; estes endereços IP de Um ou Mais Servidores Cisco ICM NT não são roteável no Internet e são para propósitos de teste somente.

Diagrama de Rede

Este documento usa a configuração de rede descrita nesta seção.

Um usuário remoto conecta ao endereço IP de Um ou Mais Servidores Cisco ICM NT do ASA com um navegador da Web SSL-permitido. Após a autenticação bem sucedida, o SVC é transferido ao computador de cliente, e o usuário pode usar uma sessão segura cifrada para o acesso direto a todos os recursos permitidos na rede corporativa.

Tarefas de Pré-configuração

Antes de iniciar, execute estas tarefas:

- Consulte Habilitação de Acesso HTTPS para o ASDM para permitir que o ASA seja configurado pelo ASDM.Para alcançar o aplicativo ASDM, de sua estação de gerenciamento, usa um navegador da Web SSL-permitido e incorpora o endereço IP de Um ou Mais Servidores Cisco ICM NT do dispositivo ASA. Por exemplo: ***inside_ip_address de https://,*** onde os *inside_ip_address* são o endereço do ASA. Uma vez que o ASDM é carregado, você pode começar a configuração do SVC.
- Transfira o pacote do cliente VPN SSL (sslclient-win*.package) do Web site da transferência de software Cisco (clientes registrados somente) ao disco rígido local da estação de gerenciamento de que você alcança o aplicativo ASDM.

O WebVPN e o ASDM não podem ser ativados na mesma interface do ASA, a menos que você altere os números de porta. Se você quer as duas Tecnologias usar a mesma porta (porta 443) no mesmo dispositivo, você pode permitir o ASDM na *interface interna* e permitir o WebVPN na *interface externa*.

Convenções

Para obter mais informações sobre das convenções de documento, refira as convenções dos dicas técnicas da Cisco.

Configurar o cliente VPN SSL em um ASA

Para configurar o cliente VPN SSL em um ASA, termine estas etapas:

1. Permita o acesso WebVPN no ASA
2. Instale e permita o cliente VPN SSL no ASA
3. Permita a instalação SVC em clientes
4. Permita Rekey parâmetros

Etapa 1. Permita o acesso WebVPN no ASA

Para permitir o WebVPN alcance no ASA, terminam estas etapas:

1. Dentro do aplicativo ASDM, clique a **configuração**, e clique então o **VPN**.
2. Expanda o **WebVPN**, e escolha o **acesso WebVPN**.
3. Selecione a relação para que você quer permitir o WebVPN, e o clique **permite.**

Etapa 2. Instale e permita o cliente VPN SSL no ASA

Para instalar e permitir o cliente VPN SSL no ASA, termine estas etapas:

1. Clique a **configuração**, e clique então o **VPN**.
2. No painel de navegação, expanda o **WebVPN**, e escolha o **cliente VPN SSL**.
3. Clique em Add.A caixa de diálogo da imagem do cliente VPN adicionar SSL aparece.
4. Clique o botão da **transferência de arquivo pela rede**.A caixa de diálogo da imagem da transferência de arquivo pela rede aparece.
5. Clique os **arquivos locais da consultação** abotoam-se para encontrar um arquivo em seu computador local, ou clicam-se o botão do **flash da consultação** para encontrar um arquivo no sistema de arquivo flash.
6. Encontre o arquivo de imagem do cliente para transferir arquivos pela rede, e clique a **APROVAÇÃO**.
7. Clique o **arquivo da transferência de arquivo pela rede**, e clique-o então **perto**.
8. Uma vez que a imagem do cliente é carregada para piscar, verifique a caixa de verificação do **cliente VPN da possibilidade SSL**, e clique-a então **aplicam-se**.**Note**: Se você recebe um Mensagem de Erro, verifique que o acesso WebVPN está permitido. No painel de navegação, expanda o **WebVPN**, e escolha o **acesso WebVPN**. Selecione a relação para que você quer configurar o acesso, e o clique **permite**.
9. Clique em **Save** e, em seguida, clique em **Yes** para aceitar as alterações.

Etapa 3. Permita a instalação SVC em clientes

Para permitir a instalação SVC em clientes, termine estas etapas:

1. No painel de navegação, expanda o **gerenciamento de endereços IP**, e escolha **associações IP**.
2. O clique **adiciona**, incorpora valores ao nome, começando o endereço IP de Um ou Mais Servidores Cisco ICM NT, terminando campos do endereço IP de Um ou Mais Servidores Cisco ICM NT, e da máscara de sub-rede. Os endereços IP de Um ou Mais Servidores Cisco ICM NT que você incorpora para o endereço IP de Um ou Mais Servidores Cisco ICM NT começando e o término de campos do endereço IP de Um ou Mais Servidores Cisco ICM NT devem vir das sub-redes em sua rede interna.
3. **A APROVAÇÃO do** clique, e clica então **aplica-se**.
4. Clique em **Save** e, em seguida, clique em **Yes** para aceitar as alterações.
5. No painel de navegação, expanda o **gerenciamento de endereços IP**, e escolha a **atribuição**.
6. Verifique a caixa de verificação das **associações do endereço interno do uso**, e então desmarcar o **Authentication Server do uso** e **use** caixas de seleção **DHCP**.
7. Clique em Apply.

8. Clique em **Save** e, em seguida, clique em **Yes** para aceitar as alterações.
9. No painel de navegação, expanda o **general**, e escolha o **grupo de túneis**.
10. Selecione o grupo de túneis que você quer controlar, e o clique **edita**.
11. Clique a aba da **atribuição de endereço de cliente**, e selecione o pool recém-criado do endereço IP de Um ou Mais Servidores Cisco ICM NT da lista disponível das associações.
12. O clique **adiciona**, e clica então a **APROVAÇÃO**.
13. No indicador do aplicativo ASDM, o clique **aplica-se**.
14. Clique em **Save** e, em seguida, clique em **Yes** para aceitar as alterações.

Etapa 4. Permita Rekey o parâmetro

Para permitir rekey parâmetros:

1. No painel de navegação, expanda o **general**, e escolha a **política do grupo**.
2. Selecione a política que você quer se aplicar a este grupo de clientes, e o clique **edita**.
3. Sob o tab geral, desmarcar os **protocolos de tunelamento herdam a** caixa de verificação, e verificam a caixa de verificação **WebVPN**.
4. Clique a aba **WebVPN**, clique a aba do **cliente SSLVPN**, e escolha estas opções:Para a opção de VPN client do uso SSL, desmarcar a caixa de verificação **herdar**, e clique o botão de rádio **opcional**.Esta escolha permite que o cliente remoto escolha mesmo se transferir o SVC. *O sempre* bem escolhido assegura-se de que o SVC esteja transferido à estação de trabalho remota durante cada conexão de VPN SSL.Para a opção Keep Installer on Client System, desmarque a caixa de seleção **Inherit** e clique no botão de opção **Yes**.Esta ação permite que o software SVC permaneça na máquina cliente; consequentemente, o ASA não está exigido para transferir o software SVC ao cliente cada vez que uma conexão é feita. Esta opção é uma boa escolha para os usuários remotos que acessam frequentemente a rede corporativa.Para a opção Renegotiation Interval, desmarque a caixa **Inherit**, desmarque a caixa de seleção **Unlimited** e insira o número de minutos até a geração de uma nova chave.A segurança é aumentada com a definição de limites no intervalo de tempo durante o qual uma chave é válida.Para a opção Renegotiation Method, desmarque a caixa de seleção **Inherit** e clique no botão de opção **SSL**. A renegociação pode utilizar o túnel SSL existente ou um túnel novo criado especificamente para a renegociação.Seus atributos do cliente VPN SSL devem ser configurados segundo as indicações desta imagem:
5. **A APROVAÇÃO do** clique, e clica então **aplica-se**.
6. Clique em **Save** e, em seguida, clique em **Yes** para aceitar as alterações.

Resultados

O ASDM cria estas configurações de linha de comando:

ciscoasa

```
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
```

Personalize sua configuração

Os procedimentos descritos dentro configuram o cliente VPN SSL em um uso ASA os nomes padrão ASA para a política do grupo (*GroupPolicy1*) e o grupo de túneis (*DefaultWebVPNGroup*) segundo as indicações desta imagem:

Este procedimento descreve como criar seus próprios políticas e grupos de túneis feitos sob encomenda do grupo e ligá-los junto de acordo com as políticas de segurança de sua organização.

Para personalizar sua configuração, termine estas etapas:

1. Crie uma política feita sob encomenda do grupo
2. Crie um grupo de túneis feito sob encomenda
3. Crie um usuário e adicionar esse usuário a sua política feita sob encomenda do grupo

Etapa 1. Crie uma política feita sob encomenda do grupo

Para criar uma política feita sob encomenda do grupo, termine estas etapas:

1. Clique a **configuração**, e clique então o **VPN**.
2. Expanda o **general**, e escolha a **política do grupo**.
3. O clique **adiciona**, e escolhe a **Política interna de grupo**.
4. No campo de nome, dê entrada com um nome para sua política do grupo.Neste exemplo, o nome da política do grupo foi mudado a *SalesGroupPolicy*.
5. Sob o tab geral, desmarcar os **protocolos de tunelamento herdam a** caixa de verificação, e verificam a caixa de verificação **WebVPN**.
6. Clique a aba **WebVPN**, e clique então a aba do **cliente SSLVPN**.Nesta caixa de diálogo, você pode igualmente fazer escolhas para o comportamento do cliente VPN SSL.
7. **A APROVAÇÃO do** clique, e clica então **aplica-se**.
8. Clique em **Save** e, em seguida, clique em **Yes** para aceitar as alterações.

Etapa 2. Crie um grupo de túneis feito sob encomenda

Para criar um grupo de túneis feito sob encomenda, termine estas etapas:

1. Clique o botão da **configuração**, e clique então o **VPN**.
2. Expanda o **general**, e escolha o **grupo de túneis**.
3. O clique **adiciona**, e escolhe o **acesso WebVPN**.
4. No campo de nome, dê entrada com um nome para seu grupo de túneis.Neste exemplo, o nome de grupo de túneis foi mudado a *SalesForceGroup*.
5. Clique a seta da gota-para baixo da **política do grupo**, e escolha sua política recém-criado do grupo.Seus política e grupo de túneis do grupo são ligados agora.

6. Clique a aba da **atribuição de endereço de cliente**, e incorpore a informação do servidor DHCP ou selecione-a de um IP pool localmente criado.
7. Clique a **APROVAÇÃO**, e clique-a então **aplicam-se**.
8. Clique em **Save** e, em seguida, clique em **Yes** para aceitar as alterações.

Etapa 3. Crie um usuário e adicionar esse usuário a sua política feita sob encomenda do grupo

Para criar um usuário e adicionar esse usuário a sua política feita sob encomenda do grupo, termine estas etapas:

1. Clique a **configuração**, e clique então o **VPN**.
2. Expanda o **general**, e escolha **usuários**.
3. O clique **adiciona**, e incorpora o nome de usuário e a informação de senha.
4. Clique a aba da **política de VPN**. Assegure-se de que seus indicadores recém-criados da política do grupo na política do grupo coloquem.Este usuário herda todas as características da política nova do grupo.
5. **A APROVAÇÃO do** clique, e clica então **aplica-se**.
6. Clique em **Save** e, em seguida, clique em **Yes** para aceitar as alterações.

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

Autenticação

A autenticação para clientes VPN SSL é realizada usando um destes métodos:

- Server do Cisco Secure ACS (raio)
- Domínio de NT
- Diretório ativo
- Senhas de uma vez
- Certificados digitais
- Carta inteligente
- Autenticação de AAA local

Esta documentação usa uma conta local criada no dispositivo ASA.

Note: Se uma ferramenta de segurança adaptável tem os pontos confiáveis múltiplos que compartilham de mesmo CA, simplesmente um destes pontos confiáveis que compartilham CA pode ser usado para validar certificados de usuário.

Configuração

Para conectar ao ASA com um cliente remoto, entre em **https://ASA_outside_address no** campo de endereço de um navegador da Web SSL-permitido. *ASA_outside_address* é o endereço IP externo de seu ASA. Se sua configuração é bem sucedida, o indicador do cliente VPN do Cisco Systems SSL aparece.

Note: O indicador do cliente VPN do Cisco Systems SSL aparece somente depois que você aceita o certificado do ASA e depois que o cliente VPN SSL está transferido à estação remota. Se o indicador não aparece, certifique-se que não se minimiza.

Comandos

Vários **comandos show** estão associados ao WebVPN. Você pode executar estes comandos na interface de linha de comando (CLI) para mostrar estatísticas e outras informações. Para informações detalhadas sobre dos **comandos show**, refira a verificação de configurações WebVPN.

Note: A Output Interpreter Tool (apenas para clientes registrados) (OIT) suporta determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

Troubleshooting

Use esta seção para resolver problemas de configuração.

Erro SVC

Problema

Você pôde receber este Mensagem de Erro durante a autenticação:

```
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
```

Solução

Se um serviço de firewall está sendo executado em seu PC, pode interromper a autenticação. Pare o serviço e reconecte o cliente.

O SVC estabeleceu uma sessão segura com o ASA?

Para assegurar o cliente VPN SSL estabeleceu uma sessão segura com o ASA:

1. **Monitoração do** clique.
2. Expanda **estatísticas de VPN**, e escolha **sessões**.
3. Do filtro pelo menu suspenso, escolha o **cliente VPN SSL**, e clique o botão do **filtro**.Sua configuração deve aparecer na lista das sessões.

As sessões seguras estão sendo estabelecidas e terminadas com sucesso?

Você pode ver os logs do tempo real para assegurar-se de que as sessões estejam sendo estabelecidas e terminadas com sucesso. Para ver logs da sessão:

1. **A monitoração do** clique, e clica então o **registro**.
2. Escolha o **Log Viewer** ou o **buffer de registro do tempo real**, e clique então a **vista**.**Note**: Para indicar somente sessões de um endereço específico, filtro pelo endereço.

Verifique o IP pool no perfil WebVPN

```
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
```

Nenhum endereço está disponível para atribuir à conexão SVC. , Atribua consequentemente o endereço do IP pool no perfil.

Se você cria o perfil da nova conexão, a seguir configurar um pseudônimo ou uma grupo-URL a fim alcançar este perfil de conexão. Se não, todas as tentativas SSL baterão o perfil da conexão VPN da Web do padrão que não teve um IP pool amarrado a ele. Ajuste isto até uso o perfil de conexão do padrão e põe um IP pool sobre ele.

Dicas

- Certifique-se de trabalhos do roteamento corretamente com o pool do endereço IP de Um ou Mais Servidores Cisco ICM NT que você atribui a seus clientes remotos. Este pool do endereço IP de Um ou Mais Servidores Cisco ICM NT deve vir de uma sub-rede em seu LAN. Você pode igualmente usar um servidor DHCP ou um Authentication Server para atribuir endereços IP de Um ou Mais Servidores Cisco ICM NT.
- O ASA cria um grupo de túneis do padrão (*DefaultWebVPNGroup*) e uma política do grupo padrão (*GroupPolicy1*). Se você cria grupos e políticas novos, certifique-se de você aplicar valores de acordo com as políticas de segurança de sua rede.
- Se você quer permitir o arquivo de Windows que consulta com CIFS, entre em um server das VITÓRIAS (NBNS) sob a **configuração > o VPN > o WebVPN > os server e as URL**. Esta tecnologia usa a seleção CIFS.

Comandos

Vários **comandos debug** estão associados ao WebVPN. Para obter informações detalhadas sobre estes comandos, consulte Uso de Comandos de Depuração do WebVPN.

Note: O uso de **comandos debug** pode afetar negativamente seu dispositivo Cisco. Antes de utilizar **comandos debug**, consulte Informações Importantes sobre Comandos Debug.

Informações Relacionadas

- Sem clientes SSL VPN (WebVPN) no exemplo de configuração ASA
- Thin client SSL VPN (WebVPN) no ASA com exemplo da configuração ASDM
- O ASA com WebVPN e escolhe Sinal-em usar o exemplo de configuração ASDM e NTLMv1
- Cisco ASA 5500 Series Adaptive Security Appliances
- Suporte Técnico e Documentação - Cisco Systems