Exemplo de Configuração de VPN SSL com Thin-Client (WebVPN) no Cisco IOS com SDM

Índice

Introdução

A tecnologia de VPN do thin client SSL pode ser usada para permitir o acesso seguro para os aplicativos que usam portas estáticas. Os exemplos são o telnet (23), o SSH (22), o POP3 (110), o IMAP4 (143), e o S TP (25). O thin client pode USER-ser conduzido, política-conduzido, ou ambos. O acesso pode ser configurado em uma base USER-por-USER, ou as políticas do grupo podem ser criadas que incluem uns ou vários usuários. A tecnologia de VPN SSL pode ser configurada em três modos principais: Sem clientes SSL VPN (WebVPN), thin client SSL VPN (transmissão da porta), e cliente VPN SSL (modo de túnel SVC-FULL).

1. **Sem clientes SSL VPN (WebVPN):**

Um cliente remoto precisa somente um navegador da Web SSL-permitido de alcançar o HTTP ou https-permitiu servidores de Web na LAN corporativa. O acesso está igualmente disponível para consultar para arquivos de Windows com o Common Internet File System (CIFS). Um bom exemplo do acesso HTTP é o cliente do acesso à Web da probabilidade (OWA).

Refira os sem clientes SSL VPN (WebVPN) no Cisco IOS usando o exemplo da configuração de SDM a fim aprender mais sobre os sem clientes SSL VPN.

2. **Thin client SSL VPN (transmissão da porta)**

Um cliente remoto deve transferir um applet pequeno, com base em Java para o acesso seguro dos aplicativos de TCP/IP que usam números de porta estática. O UDP não é apoiado. Os exemplos incluem o acesso ao POP3, ao S TP, ao IMAP, ao SSH, e ao telnet. Os privilégios administrativos locais das necessidades de usuário porque as mudanças são feitas aos arquivos na máquina local. Este método de SSL VPN não trabalha com aplicativos que usam atribuições de porta dinâmica, por exemplo, diversos aplicativos de FTP.

3. **Cliente VPN SSL (modo de túnel SVC-FULL):**

O cliente VPN SSL transfere um cliente pequeno à estação de trabalho remota e permite-o completamente, acesso seguro aos recursos na rede corporativa interna. O SVC pode ser transferido permanentemente à estação remota, ou pode ser removido após as extremidades seguras da sessão.

Refira o cliente VPN SSL (SVC) em IO usando o exemplo da configuração de SDM a fim aprender mais sobre o cliente VPN SSL.

Este documento demonstra uma configuração simples para o thin client SSL VPN em um roteador do ® do Cisco IOS. O thin client SSL VPN é executado neste Roteadores do Cisco IOS:

- Cisco 870, 1811, 1841, 2801, 2811, 2821, e 2851 Series Router
- Cisco 3725, 3745, 3825, 3845, 7200, e 7301 Series Router

Pré-requisitos

Requisitos

Certifique-se de atender a estes requisitos antes de tentar esta configuração:

Exigências para o roteador do Cisco IOS

- Algum do Roteadores listado carregado com o SDM e uma imagem avançada Versão do IOS de 12.4(6)T ou de mais tarde
- Estação de gerenciamento carregada com o SDMRoteadores novo dos navios de Cisco com uma cópia instalada do SDM. Se seu roteador não tem o SDM instalado, você pode obter o software no Security Device Manager de Transferência-Cisco do software. Você deve possuir uma conta CCO com um contrato de serviço. Consulte para configurar seu roteador com o Security Device Manager para instruções detalhadas.

Exigências para computadores de cliente

- Os clientes remotos devem ter privilégios administrativos locais; não se exige, mas sugere-se altamente.
- Os clientes remotos devem ter a versão 1.4 ou mais recente do ambiente de tempo de execução de java (JRE).
- Navegadores de cliente remoto: Internet explorer 6.0, Netscape 7.1, Mozilla 1.7, safari 1.2.2, ou Firefox 1.0
- Cookie permitidos e pop-up permitidos em clientes remotos

Componentes Utilizados

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

- Cisco avançou a imagem 12.4(9)T do software de empreendimento
- Roteador de serviços integrados Cisco 3825
- Versão 2.3.1 de Roteador Cisco e Security Device Manager (SDM)

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos usados neste documento começaram com uma configuração limpa (padrão). Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando. Os endereços IP de Um ou Mais Servidores Cisco ICM NT usados para esta configuração vêm do espaço de endereços do RFC 1918. Não são legais no Internet.

Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Configurar

Tarefa

Esta seção contém a informação necessária configurar as características descritas dentro deste documento.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:

Configurar o thin client SSL VPN

Use o assistente fornecido na relação do Security Device Manager (SDM) para configurar o thin client SSL VPN no Cisco IOS, ou configurar-lo no comando line interface(cli) ou manualmente no aplicativo SDM. Este exemplo usa o assistente.

1. Escolha a aba **configurar**.Do painel de navegação, escolha **VPN > WebVPN**.Clique a aba da **criação WebVPN**.Clique o botão de rádio ao lado de **criam um WebVPN novo**.Clique o **lançamento o** botão de **tarefa selecionado**.
2. Os lançamentos do assistente WebVPN. Clique em Next.Dê entrada com o endereço IP de Um ou Mais Servidores Cisco ICM NT e um nome exclusivo para este gateway WebVPN. Clique em Next.
3. A tela de autenticação de usuário permite a oportunidade de prever a autenticação dos usuários. Esta configuração usa uma conta criada localmente no roteador. Você pode igualmente usar um server do Authentication, Authorization, and Accounting (AAA).Para adicionar um usuário, o clique **adiciona**.Incorpore a informação sobre o usuário adicionar uma tela da conta, e clique a **APROVAÇÃO**.Clique **em seguida na** tela de autenticação de usuário.A tela de wizard WebVPN permite a configuração de sites do intranet, mas esta etapa é omitida porque a Porta-transmissão é usada para este acesso de aplicativo. Se você quer permitir o acesso aos sites, use os sem clientes ou as configurações de VPN completas

do cliente SSL, que não são no âmbito deste documento.Clique em Next. O assistente indica uma tela que permita a configuração do cliente completo do túnel. Isto não se aplica ao thin client SSL VPN (transmissão da porta).Desmarcar **permitem o túnel completo**. Clique em Next.

4. Personalize a aparência da página portal WebVPN ou aceite a aparência do padrão.Clique em Next.Inspecione o sumário da configuração e clique o **revestimento > a salvaguarda**.
5. Você criou um gateway WebVPN e um contexto WebVPN com uma política ligada do grupo. Configurar as portas do thin client, que estão feitas disponíveis quando os clientes conectam ao WebVPN.Escolha **configuram**.Escolha **VPN > WebVPN**.Escolha **criam o WebVPN**.Escolha o botão de rádio **configuram recursos avançados para um WebVPN existente** e clicam o **lançamento a tarefa selecionada**.A tela de boas vindas oferece destaques das capacidades do assistente. Clique em Next.Escolha o contexto e o grupo de usuário WebVPN dos menus suspensos. Clique em Next.Escolha o **thin client (transmissão da porta)** e clique-o **em seguida**.Incorpore os recursos que você quer fazer a transmissão direta disponível da porta. A porta do serviço deve ser uma porta estática, mas você pode aceitar a porta padrão no PC cliente atribuído pelo assistente. Clique em Next.Inspecione seu sumário de configuração e clique o **revestimento > APROVADO > salvaguarda**.

Configuração

Resultados da configuração de SDM.

ausnml-3825-01

```
Building configuration...

Current configuration : 4343 bytes
!
! Last configuration change at 15:55:38 UTC Thu Jul 27
2006 by ausnml
! NVRAM config last updated at 21:30:03 UTC Wed Jul 26
2006 by ausnml
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname ausnml-3825-01
!
boot-start-marker
boot system flash c3825-adventerprisek9-mz.124-9.T.bin
boot-end-marker
!
no logging buffered
enable secret 5 $1$KbIu$5o8qKYAVpWvyv9rYbrJLi/
!
aaa new-model
!
aaa authentication login default local
aaa authentication login sdm_vpn_xauth_ml_1 local
aaa authentication login sdm_vpn_xauth_ml_2 local
aaa authorization exec default local
!
aaa session-id common
!
```

```
resource policy
!
ip cef
!
ip domain name cisco.com
!
voice-card 0
 no dspfarm
!--- Self-Signed Certificate Information crypto pki
trustpoint ausnml-3825-01_Certificate enrollment
selfsigned serial-number none ip-address none
revocation-check crl rsakeypair ausnml-3825-
01_Certificate_RSAKey 1024 ! crypto pki certificate
chain ausnml-3825-01_Certificate certificate self-signed
02 30820240 308201A9 A0030201 02020102 300D0609 2A864886
F70D0101 04050030 !---------------------- !--- cut for
brevity quit ! username ausnml privilege 15 password 7
15071F5A5D292421 username fallback privilege 15 password
7 08345818501A0A12 username austin privilege 15 secret 5
$1$3xFv$W0YUsKDx1adDc.cVQF2Ei0 username sales_user1
privilege 5 secret 5 $1$2/SX$ep4fsCpodeyKaRji2mJkX/
username admin0321 privilege 15 secret 5
$1$FxzG$cQUJeUpBWgZ.scSzOt8Ro1 ! interface
GigabitEthernet0/0 ip address 192.168.0.37 255.255.255.0
duplex auto speed auto media-type rj45 ! interface
GigabitEthernet0/1 ip address 172.22.1.151 255.255.255.0
duplex auto speed auto media-type rj45 ! ip route
0.0.0.0 0.0.0.0 172.22.1.1 ! ip http server ip http
authentication local ip http secure-server ip http
timeout-policy idle 600 life 86400 requests 100 !
control-plane ! line con 0 stopbits 1 line aux 0
stopbits 1 line vty 0 4 exec-timeout 40 0 privilege
level 15 password 7 071A351A170A1600 transport input
telnet ssh line vty 5 15 exec-timeout 40 0 password 7
001107505D580403 transport input telnet ssh ! scheduler
allocate 20000 1000 !--- the WebVPN Gateway webvpn
gateway gateway_1 ip address 192.168.0.37 port 443 http-
redirect port 80 ssl trustpoint ausnml-3825-
01_Certificate inservice !--- the WebVPN Context webvpn
context webvpn title-color #CCCC66 secondary-color white
text-color black ssl authenticate verify all !---
resources available to the thin-client port-forward
"portforward_list_1" local-port 3002 remote-server
"172.22.1.20" remote-port 110 description "Pop3 Email"
local-port 3001 remote-server "172.22.1.30" remote-port
23 description "Router1" local-port 3000 remote-server
"172.22.1.50" remote-port 25 description "Email" local-
port 3003 remote-server "172.22.1.10" remote-port 22
description "Router2 SSH" !--- the group policy policy
group policy_1 port-forward "portforward_list_1"
default-group-policy policy_1 aaa authentication list
sdm_vpn_xauth_ml_2 gateway gateway_1 domain webvpn max-
users 2 inservice ! end
```

Verificar

Verifique sua configuração

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

1. Use um computador de cliente para alcançar o gateway WebVPN em **https://gateway_ip_address.** Recorde incluir o Domain Name WebVPN se você cria contextos originais WebVPN. Por exemplo, se você criou um domínio chamado vendas, entre em **https://gateway_ip_address/sales**.
2. Entre e aceite o certificado oferecido pelo gateway WebVPN. Clique o **acesso de aplicativo do começo**.
3. Displays de tela de um acesso de aplicativo. Você pode alcançar um aplicativo com o número de porta local e seu endereço IP de Um ou Mais Servidores Cisco ICM NT do loopback local. Por exemplo, ao telnet ao roteador1, entre no **telnet 127.0.0.1 3001**. O Java applet pequeno envia esta informação ao gateway WebVPN, que amarra então os dois fins da sessão junto em uma forma segura. As conexões bem sucedidas podem fazer com que os **bytes para fora** e os **bytes nas** colunas aumentem.

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 ver em detalhe o uso dos **comandos show**, refira a verificação da configuração WebVPN.

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.

Os computadores de cliente devem ser carregados com a versão 1.4 ou mais recente das Javas do SOL. Obtenha uma cópia deste software do download do software das Javas

Comandos usados para pesquisar defeitos

Nota: Refira a informação importante em comandos Debug antes do uso dos **comandos debug**.

- **mostre o webvpn?** — Há muitos **comandos show** associados com o WebVPN. Estes podem ser executados no CLI para mostrar estatísticas e a outra informação. A fim ver em detalhe o uso dos **comandos show**, refira a verificação da configuração WebVPN.
- **debugar o webvpn?** — O uso dos **comandos debug** pode adversamente impactar o roteador. A fim ver com maiores detalhes o uso dos **comandos debug**, refira a utilização de comandos Debug WebVPN.

Informações Relacionadas

- Cisco IOS SSLVPN
- SSL VPN - WebVPN
- Cisco IOS WebVPN Q&A
- Suporte Técnico e Documentação - Cisco Systems