O ASA com WebVPN e escolhe Sinal-em usar o exemplo de configuração ASDM e NTLMv1

Índice

Introdução

Este documento descreve como configurar o Cisco Adaptive Security Appliance (ASA) para passar automaticamente as credenciais de login do usuário WebVPN, assim como a autenticação secundária, para servidores que exigem uma validação de login adicional contra o Windows Active Directory que executa o NT LAN Manager version 1 (NTLMv1). Esta característica é conhecido como login único (SSO). Ele fornece aos links configurados para um grupo específico de WebVPN a capacidade de passar sobre estas informações de autenticação de usuário, eliminando assim várias solicitações de autenticação. Esta característica também pode ser usada no nível global ou de configuração de usuário.

Pré-requisitos

Requisitos

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

- Assegure-se de que o NTLMv1 e as permissões de Windows para os usuários do alvo VPN estejam configurados. Consulte sua documentação Microsoft para obter mais informações sobre dos direitos de acesso do domínio do Windows.

Componentes Utilizados

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

- Cisco ASA 7.1(1)
- Cisco Adaptive Security Device Manager (ASDM) 5.1(2)
- Internet Information Services de Microsoft (IIS)

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

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

Configurar

Nesta seção, você é presentado com a informação para configurar o ASA como um servidor VPN da Web com SSO.

Nota: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

Adicionar um servidor AAA para a autenticação do domínio do Windows

Termine estas etapas para configurar o ASA para usar um controlador de domínio para a autenticação.

1. Selecione a **configuração > as propriedades > o AAA Setup > servidores AAA** e o clique **adiciona**. Forneça um nome para o grupo de servidor, tal como Windows_NT, e escolha o **domínio de NT** como o protocolo.
2. Adicionar um Windows Server.Selecione o grupo recém-criado e o clique **adiciona**. Selecione a relação onde o server é encontrado e dê entrada com o endereço IP de Um ou Mais Servidores Cisco ICM NT e o nome do controlador de domínio. Seja certo que o nome do controlador de domínio está dado entrada com em todas as letras maiúsculas. Clique a **APROVAÇÃO** quando você é feito.Este indicador mostra a configuração de AAA terminada:

Crie um certificado auto-assinado

Termine estas etapas para configurar o ASA para usar um certificado auto-assinado.

Nota: Neste exemplo um certificado auto-assinado é usado para a simplicidade. Para outras opções do certificado de registro, tais como registrar-se com um Certificate Authority externo, refira configurar Certificados.

1. Selecione a **configuração > as propriedades > o certificado > o ponto confiável > a configuração** e o clique **adiciona**.
2. No indicador que aparece dê entrada com um nome do ponto confiável tal como o Local-TP e a verificação **gerenciem um certificado auto-assinado no registro**. As outras opções podem ser deixadas com suas configurações padrão. **APROVAÇÃO do** clique quando você for feito.Este indicador mostra a configuração terminada do ponto confiável:

Permita o WebVPN na interface externa

Termine estas etapas para permitir que os usuários fora de sua rede conectem usando o WebVPN.

1. Selecione a **configuração > o VPN > o WebVPN > o acesso WebVPN**.
2. Selecione a interface desejada, o clique **permite**, e a verificação **permite a lista de drop-down do grupo de túneis na página de login WebVPN**.**Nota:** Se a mesma relação é usada para o acesso WebVPN e ASDM, você deve mudar a porta padrão para o acesso ASDM da porta 80 a uma porta nova tal como 8080. Isto é feito sob a **configuração > as propriedades > o acesso de dispositivo > o HTTPS/ASDM.Nota:** Você pode automaticamente reorientar um usuário à porta 443 caso um usuário navegar ao **<ip_address> de http://** em vez do **<ip_address> de https://**. Selecione a **configuração > as propriedades > o HTTP/HTTPS**, escolha a interface desejada, o clique **edita** e seleto **reoriente o HTTP ao HTTPS**.

Configurar uma lista URL para seus server internos

Termine estas etapas para criar uma lista que contenha os server para que você quer conceder seu acesso de usuários WebVPN.

1. Selecione a **configuração > o VPN > o WebVPN > os server e as URL** e o clique **adicionam**.
2. Dê entrada com um nome para a lista URL. Este nome não é visível aos utilizadores finais. Clique em Add.
3. Dê entrada com o nome do indicador URL porque deve ser indicada aos usuários. Incorpore a informação de URL do server. Isto deve ser como você alcança normalmente o server.
4. Clique a **APROVAÇÃO**, **APROVAÇÃO**, e **aplique-a** então.

Configurar uma Política interna de grupo

Termine estas etapas para configurar uma política do grupo para seus usuários WebVPN.

1. Selecione a **configuração > o VPN > a política do general > do grupo**, o clique **adiciona**, e seleciona a **Política interna de grupo**.
2. No tab geral, especifique um nome da política, tal como Internal-Group_POL_WEBVPN. Desmarcar então **herdam** ao lado dos protocolos de tunelamento e da verificação **WebVPN**.
3. Na aba WebVPN selecione a **outra secundário-**aba. Desmarcar **herdam** ao lado dos server e das listas URL e selecionam a lista URL que você configurou da lista de drop-down. Clique a

APROVAÇÃO quando você é feito.

Configurar um grupo de túneis

Termine estas etapas para configurar um grupo de túneis para seus usuários WebVPN.

1. Selecione a **configuração > o VPN > o general > o grupo de túneis**, o clique **adiciona** e seleciona o **acesso WebVPN…**
2. Dê entrada com um nome para o grupo de túneis, tal como WEB_VPN-GRP. Na aba básica selecione a política do grupo que você criou e verifique que o tipo de grupo é **webvpn**.
3. Vá à aba AAA.Para o grupo de Authentication Server, escolha o grupo que você configurou a fim permitir a autenticação NTLMv1 com seu controlador de domínio.**Opcional:** Verifique o **LOCAL do uso se o grupo de servidor** não permite o uso da base de dados de usuário local caso o grupo configurado AAA falhar. Isto pode ajudá-lo a pesquisar defeitos mais tarde.
4. Vá à aba WebVPN e vá então à secundário-aba dos **pseudônimos e URL do grupo**.
5. Incorpore um pseudônimo sob pseudônimos do grupo e o clique **adiciona**. Este pseudônimo aparece na lista de drop-down apresentada aos usuários WebVPN no início de uma sessão.
6. Clique em **OK** e, em seguida, em **Apply**.

Configurar o Auto-Signon para um server

Comute à linha de comando para permitir o SSO para seus server internos.

Nota: Esta etapa não pode ser terminada no ASDM e deve ser realizada usando a linha de comando. Refira o acesso da interface de linha de comando para mais informação.

Use o **comando auto-signon** especificar os recursos de rede, tais como um server, que você quer dar seu acesso de usuários a. Um endereço IP de Um ou Mais Servidores Cisco ICM NT do servidor único é configurado aqui, mas um intervalo de rede tal como **10.1.1.0 /24** pode igualmente ser especificado. Refira o comando auto-signon para mais informação.

```
ASA>enable ASA#configure terminal ASA(config)#webvpn ASA(config-webpvn)#auto-signon allow ip
10.1.1.200 255.255.255.255 auth-type ntlm ASA(config-webvpn)#quit ASA(config)#exit ASA#write
memory
```

Nestas saídas de exemplo, o **comando auto-signon** é configurado para o WebVPN globalmente. Este comando pode igualmente ser usado no modo da configuração de grupo WebVPN ou no modo de configuração do nome de usuário de VPN da Web. O uso deste comando no modo da configuração de grupo WebVPN limita-o a um grupo particular. Igualmente, o uso deste comando no modo de configuração do nome de usuário de VPN da Web limita-o a um usuário individual. Refira o comando auto-signon para mais informação.

Configuração ASA final

Este documento utiliza esta configuração:

Versão ASA 7.1(1)

```
ASA#show running-config : Saved : ASA Version 7.1(1) !
terminal width 200 hostname ASA domain-name cisco.com
enable password 8Ry2YjIyt7RRXU24 encrypted names !
interface GigabitEthernet0/0 nameif outside security-
level 0 ip address 172.16.171.51 255.255.255.0 !
```

```
interface GigabitEthernet0/1 nameif inside security-
level 100 ip address 10.1.1.1 255.255.255.0 ! interface
GigabitEthernet0/2 shutdown no nameif no security-level
no ip address ! interface GigabitEthernet0/3 shutdown no
nameif no security-level no ip address ! interface
Management0/0 shutdown no nameif no security-level no ip
address ! passwd 2KFQnbNIdI.2KYOU encrypted ftp mode
passive dns server-group DefaultDNS domain-name
cisco.com pager lines 24 mtu inside 1500 mtu outside
1500 no failover asdm image disk0:/asdm512.bin no asdm
history enable arp timeout 14400 route outside 0.0.0.0
0.0.0.0 172.16.171.1 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 timeout mgcp-pat 0:05:00 sip 0:30:00
sip_media 0:02:00 timeout uauth 0:05:00 absolute !---
AAA server configuration aaa-server Windows_NT protocol
nt aaa-server Windows_NT host 10.1.1.200 nt-auth-domain-
controller ESC-SJ-7800 !--- Internal group policy
configuration group-policy Internal-GRP_POL_WEBVPN
internal group-policy Internal-GRP_POL_WEBVPN attributes
vpn-tunnel-protocol webvpn webvpn url-list value
webserver username cisco password Q/odgwmtmVIw4Dcm
encrypted privilege 15 aaa authentication http console
LOCAL aaa authentication ssh console LOCAL aaa
authentication enable console LOCAL http server enable
8181 http 0.0.0.0 0.0.0.0 outside no snmp-server
location no snmp-server contact snmp-server enable traps
snmp authentication linkup linkdown coldstart !---
Trustpoint/certificate configuration crypto ca
trustpoint Local-TP enrollment self crl configure crypto
ca certificate chain Local-TP certificate 31 308201b0
30820119 a0030201 02020131 300d0609 2a864886 f70d0101
04050030 1e311c30 1a06092a 864886f7 0d010902 160d4153
412e6369 73636f2e 636f6d30 1e170d30 36303333 30313334
3930345a 170d3136 30333237 31333439 30345a30 1e311c30
1a06092a 864886f7 0d010902 160d4153 412e6369 73636f2e
636f6d30 819f300d 06092a86 4886f70d 01010105 0003818d
00308189 02818100 e47a29cd 56becf8d 99d6d919 47892f5a
1b8fc5c0 c7d01ea6 58f3bec4 a60b2025 03748d5b 1226b434
561e5507 5b45f30e 9d65a03f 30add0b5 81f6801a 766c9404
9cabcbde 44b221f9 b6d6dc18 496fe5bb 4983927f adabfb17
68b4d22c cddfa6c3 d8802efc ec3af7c7 749f0aa2 3ea2c7e3
776d6d1d 6ce5f748 e4cda3b7 4f007d4f 02030100 01300d06
092a8648 86f70d01 01040500 03818100 c6f87c61 534bb544
59746bdb 4e01680f 06a88a15 e3ed8929 19c6c522 05ec273d
3e37f540 f433fb38 7f75928e 1b1b6300 940b8dff 69eac16b
af551d7f 286bc79c e6944e21 49bf15f3 c4ec82d8 8811b6de
775b0c57 e60a2700 fd6acc16 a77abee6 34cb0cad 81dfaf5a
f544258d cc74fe2d 4c298076 294f843a edda3a0a 6e7f5b3c
quit !--- Tunnel group configuration tunnel-group
WEB_VPN-GRP type webvpn tunnel-group WEB_VPN-GRP
general-attributes authentication-server-group
Windows_NT default-group-policy Internal-GRP_POL_WEBVPN
tunnel-group WEB_VPN-GRP webvpn-attributes group-alias
Group-Selection enable telnet timeout 5 ssh timeout 5
console timeout 0 ! class-map inspection_default match
default-inspection-traffic ! ! policy-map global_policy
class inspection_default inspect dns maximum-length 512
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 ! service-policy global_policy global
!--- WebVPN Configuration webvpn enable outside url-list
```

```
webserver "Internal Server" https://10.1.1.200 1 tunnel-
group-list enable auto-signon allow ip 10.1.1.200
255.255.255.255 auth-type ntlm
Cryptochecksum:c80ac5f6232df50fc1ecc915512c3cd6 : end
```

Verificar

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

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.

Teste um início de uma sessão WebVPN

Entre como um usuário para testar sua configuração.

1. Tente entrar ao ASA com informação sobre o usuário de seu domínio de NT. Selecione o grupo configurado aliás na etapa 5 configuram abaixo um grupo de túneis.
2. Procure os links configurados aos server internos. Clique sobre o link para verificar.

Sessões de monitor

Selecione a **monitoração > o VPN > as estatísticas de VPN > as sessões** e procure uma sessão de VPN da Web que pertença ao grupo configurado neste documento.

Debugar uma sessão de VPN da Web

Esta saída é uma amostra debuga de uma sessão de VPN da Web bem-sucedida.

Nota: Consulte Informações Importantes sobre Comandos de Depuração antes de usar comandos **debug**.

```
ASA#debug webvpn 255 INFO: debug webvpn enabled at level 255 ASA# ASA#
webvpn_portal.c:ewaFormServe_webvpn_login[1570] webvpn_portal.c:http_webvpn_kill_cookie[385]
webvpn_auth.c:webvpn_auth[286] WebVPN: no cookie present!!
webvpn_portal.c:ewaFormSubmit_webvpn_login[1640] webvpn_portal.c:http_webvpn_kill_cookie[385]
webvpn_auth.c:http_webvpn_pre_authentication[1782] !--- Begin AAA WebVPN: calling AAA with
ewsContext (78986968) and nh (78960800)! WebVPN: started user authentication...
webvpn_auth.c:webvpn_aaa_callback[3422] WebVPN: AAA status = (ACCEPT)
webvpn_portal.c:ewaFormSubmit_webvpn_login[1640]
webvpn_auth.c:http_webvpn_post_authentication[1095] WebVPN: user: (test) authenticated. !--- End
AAA webvpn_auth.c:http_webvpn_auth_accept[2093] webvpn_session.c:http_webvpn_create_session[159]
webvpn_session.c:http_webvpn_find_session[136] WebVPN session created!
webvpn_session.c:http_webvpn_find_session[136] webvpn_db.c:webvpn_get_server_db_first[161]
webvpn_db.c:webvpn_get_server_db_next[202] traversing list: (webserver)
webvpn_portal.c:ewaFormServe_webvpn_cookie[1421] webvpn_auth.c:webvpn_auth[286]
webvpn_session.c:http_webvpn_find_session[136] webvpn_session.c:webvpn_update_idle_time[924]
WebVPN: session has been authenticated. webvpn_auth.c:webvpn_auth[286]
webvpn_session.c:http_webvpn_find_session[136] webvpn_session.c:webvpn_update_idle_time[924]
WebVPN: session has been authenticated. !--- Output supressed webvpn_auth.c:webvpn_auth[286]
webvpn_session.c:http_webvpn_find_session[136] webvpn_session.c:webvpn_update_idle_time[924]
WebVPN: session has been authenticated. webvpn_auth.c:webvpn_auth[286]
webvpn_session.c:http_webvpn_find_session[136] webvpn_session.c:webvpn_update_idle_time[924]
WebVPN: session has been authenticated. webvpn_auth.c:webvpn_auth[286]
webvpn_session.c:http_webvpn_find_session[136] webvpn_session.c:webvpn_update_idle_time[924]
```

```
WebVPN: session has been authenticated. webvpn_auth.c:webvpn_auth[286]
webvpn_session.c:http_webvpn_find_session[136] webvpn_session.c:webvpn_update_idle_time[924]
WebVPN: session has been authenticated. webvpn_auth.c:webvpn_auth[286]
webvpn_session.c:http_webvpn_find_session[136] webvpn_session.c:webvpn_update_idle_time[924]
WebVPN: session has been authenticated. webvpn_session.c:http_webvpn_find_session[136]
webvpn_session.c:webvpn_update_idle_time[924]
```

Troubleshooting

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

- Se a caixa suspensa do grupo não está atual na página de login WebVPN, seja certo que você terminou etapa 2 permite abaixo o WebVPN na interface externa e a etapa 5 configura abaixo um grupo de túneis. Se estas etapas não são terminadas e a gota-para baixo falta, a autenticação cai sob o grupo padrão e falha provavelmente.
- Embora você não possa atribuir direitos de acesso ao usuário no ASDM ou no ASA, você pode restringir usuários com os direitos de acesso de Microsoft Windows em seu controlador de domínio. Adicionar as permissões necessárias do grupo de NT para o página da web que o usuário autentica a. Uma vez os log de usuário no WebVPN com as permissões do grupo, acesso às páginas especificadas são concedidos ou negados em conformidade. O ASA atua somente como um host da autenticação de proxy em nome do controlador de domínio e todas as comunicações aqui são NTLMv1.
- Você não pode configurar o SSO para Sharepoint sobre o WebVPN porque o server de Sharepoint não apoia a autenticação baseada formulários. Em consequência, os endereços da Internet com cargo ou o procedimento de encaixe do cargo não são aplicáveis aqui.

Informações Relacionadas

- Cisco ASA 5500 Series Adaptive Security Appliances
- Suporte Técnico e Documentação - Cisco Systems