PIX/ASA 7.x: Exemplo de Configuração de Habilitação de Serviços de FTP/TFTP

Índice

Introdução

Este documento explica os passos necessários para os usuários fora de sua rede acessarem serviços de FTP e TFTP em sua rede DMZ.

File Transfer Protocol (FTP)

Há duas formas de FTP:

- Modo ativo
- Modo passivo

No modo de FTP ativo, o cliente se conecta de uma porta sem privilégios aleatória (N > 1023) à porta de comandos (21) do servidor FTP. Em seguida, o cliente começa a escutar a porta N+1 e envia a porta de comandos de FTP N+1 para o servidor. O servidor então se conecta de volta às portas de dados especificadas do cliente com sua porta de dados local, a porta 20.

No modo de FTP passivo, o cliente inicia ambas as conexões para o servidor, o que resolve o problema de um firewall que filtra a conexão da porta de dados de entrada para o cliente do servidor. Quando uma conexão de FTP é aberta, o cliente abre duas portas não privilegiadas aleatórias localmente (N > 1023 e N+1). A primeira porta contacta o server na porta 21. Mas em vez então de emitir um **comando port** e de permitir que o server conecte de volta a seus dados mova, os problemas de cliente o **comando pasv**. O resultado é que o servidor abre uma porta não privilegiada aleatória (P > 1023) e envia o comando **port P** para o cliente. O cliente então inicia a conexão da porta N+1 para a porta P no servidor para transferir os dados. Sem o comando de configuração **inspection** no Security Appliance, o FTP de usuários internos direcionado para fora da rede funciona somente no modo passivo. Além disso, os usuários externos que tentarem acessar seu servidor FTP interno terão o acesso negado.

Refira ASA 8.3 e mais atrasado: Permita o exemplo de configuração dos serviços FTP/TFTP para obter mais informações sobre da configuração idêntica usando o ASDM com a ferramenta de segurança adaptável de Cisco (ASA) com versão 8.3 e mais recente.

Trivial File Transfer Protocol (TFTP)

O TFTP, conforme descrito na RFC 1350, é um protocolo simples para ler e gravar arquivos entre um servidor e um cliente TFTP. O TFTP usa a porta 69 do UDP.

Pré-requisitos

Requisitos

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

- Uma comunicação básica foi estabelecida entre as interfaces necessárias.
- Você possui um servidor FTP configurado em sua rede DMZ.

Componentes Utilizados

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

- ASA 5500 Series Adaptive Security Appliance com imagem de software 7.2(2)
- Windows 2003 Server com serviços de FTP
- Windows 2003 Server com serviços de TFTP
- PC cliente localizado fora da rede

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.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:

Nota: Os esquemas de endereçamento IP usados nesta configuração não são legalmente roteáveis na Internet. São os endereços da RFC1918 que foram usados em um ambiente de laboratório.

Produtos Relacionados

Esta configuração também pode ser usada com o PIX Security Appliance 7.x.

Convenções

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

Informações de Apoio

O Security Appliance oferece suporte à inspeção de aplicativos por meio da função Adaptive Security Algorithm. Ao usar a inspeção stateful de aplicativos do Adaptive Security Algorithm, o Security Appliance controla todas as conexões que cruzam o firewall e garante que elas sejam válidas. O firewall, por meio da inspeção stateful, também monitora o estado da conexão para compilar informações e colocá-las em uma tabela de estados. Com o uso da tabela de estados além das regras definidas pelo administrador, as decisões de filtragem baseiam-se no contexto que é estabelecido pelos pacotes transmitidos previamente pelo firewall. A implementação de inspeções de aplicativos consiste nas seguintes ações:

- Identificar o tráfego.
- Aplicar inspeções ao tráfego.
- Ativar as inspeções em uma interface.

Gerenciamento Avançado de Protocolos

FTP

Alguns aplicativos necessitam de gerenciamento especial pelas funções de inspeção de aplicativos do Cisco Security Appliance. Esses tipos de aplicativos normalmente incorporam informações de endereçamento IP no pacote de dados do usuário ou abrem canais secundários em portas atribuídas dinamicamente. A função de inspeção de aplicativos funciona com o Network Address Translation (NAT) para ajudar a identificar o local das informações de endereçamento incorporadas.

Além da identificação das informações de endereçamento incorporadas, a função de inspeção de aplicativos monitora as sessões para determinar os números de porta para canais secundários. Muitos protocolos abrem portas TCP ou UDP secundárias para aprimorar o desempenho. A sessão inicial em uma porta bem conhecida é usada para negociar números de portas atribuídos dinamicamente. A função de inspeção de aplicativos monitora essas sessões, identifica as atribuições de portas dinâmicas e permite a troca de dados nessas portas pela duração das sessões específicas. Aplicativos multimídia e de FTP exibem esse tipo de comportamento.

O protocolo FTP necessita de algum gerenciamento especial porque usa duas portas por sessão de FTP. O protocolo de FTP usa duas portas quando ativado para dados de transferência: um canal de controle e um canal de dados que use a porta 21 e 20, respectivamente. O usuário, que inicia a sessão de FTP via canal de controle, faz todas as solicitações de dados por meio desse canal. O servidor FTP então inicia uma solicitação para abrir uma porta da porta 20 do servidor para o computador do usuário. O FTP sempre usa a porta 20 para comunicações do canal de dados. Se a inspeção de FTP não tiver sido habilitada no Security Appliance, esta solicitação será

descartada e as sessões de FTP não transmitirão nenhum dado solicitado. Se a inspeção de FTP estiver habilitada no Security Appliance, o Security Appliance irá monitorar o canal de controle e tentará reconhecer uma solicitação de abertura do canal de dados. O protocolo FTP incorpora as especificações de porta do canal de dados no tráfego do canal de controle, o que exige que o Security Appliance inspecione o canal de controle em busca de alterações nas portas de dados. Se o Security Appliance reconhecer uma solicitação, ele criará temporariamente uma abertura para o tráfego do canal de dados que durará até o final da vida útil da sessão. Desta forma, a função de inspeção de FTP monitora o canal de controle, identifica uma atribuição de porta de dados e permite que os dados sejam trocados na porta de dados durante a sessão.

Por padrão, o Security Appliance inspeciona as conexões da porta 21 para tráfego FTP por meio do mapa de classes de inspeção global. O Security Appliance também reconhece a diferença entre sessões de FTP ativas e passivas. Se as sessões de FTP oferecerem suporte à transferência de dados de FTP no modo passivo, o Security Appliance, via comando **inspect ftp**, reconhecerá a solicitação de porta de dados do usuário e abrirá uma nova porta superior à 1023.

A inspeção de aplicativos de FTP inspeciona as sessões de FTP e executa quatro tarefas:

- Prepara uma conexão de dados secundária dinâmica.
- Acompanha a seqüência de comandos e respostas do FTP.
- Gera uma trilha de auditoria.
- Converte os endereços IP incorporados usando o NAT.

A inspeção de aplicativos de FTP prepara os canais de dados secundários para a transferência de dados de FTP. Os canais são alocados em resposta a um upload de arquivo, a um download de arquivo ou a um evento de listagem de diretório, e todos devem ser pré-negociados. A porta é negociada por meio dos comandos **PORT** ou **PASV** (227).

TFTP

A inspeção de TFTP é habilitada por padrão.

O Security Appliance inspeciona o tráfego de TFTP e cria dinamicamente conexões e conversões e, se necessário, permite a transferência de arquivos entre um cliente e um servidor TFTP. Especificamente, o mecanismo de inspeção inspeciona solicitações de leitura (RRQ), solicitações de gravação (WRQ) e notificações de erro (ERROR) do TFTP.

Um canal secundário dinâmico e uma conversão PAT, se necessários, são alocados mediante o recebimento de uma RRQ ou WRQ válida. Este canal secundário é subseqüentemente usado pelo TFTP para a transferência de arquivos ou a notificação de erros.

Somente o servidor TFTP pode iniciar o tráfego via canal secundário, e no máximo um canal secundário incompleto pode existir entre o cliente e o servidor TFTP. Uma notificação de erro do servidor fecha o canal secundário.

A inspeção de TFTP deverá ser habilitada se o PAT estático for usada para redirecionar o tráfego de TFTP.

Configuração da Inspeção Básica de Aplicativos de FTP

Por padrão, a configuração inclui uma política que corresponde a todo o tráfego de inspeção de aplicativos padrão e aplica a inspeção ao tráfego em todas as interfaces (uma política global). O

tráfego de inspeção de aplicativos padrão inclui o tráfego para as portas padrão para cada protocolo. É possível aplicar somente uma política global. Assim, se desejar alterar a política global, por exemplo, para aplicar inspeção a portas não padrão ou adicionar inspeções que não são habilitadas por padrão, você deverá editar a política padrão ou desabilitá-la e aplicar uma nova política. Para obter uma lista de todas as portas padrão, consulte Política de Inspeção Padrão.

1. Execute o comando **policy-map global_policy**.`ASAwAIP-CLI(config)#policy-map global_policy`
2. Execute o comando **class inspection_default**.`ASAwAIP-CLI(config-pmap)#class inspection_default`
3. Execute o comando **inspect FTP**.`ASAwAIP-CLI(config-pmap-c)#inspect FTP` Há a opção de usar o comando **inspect FTP strict**. Esse comando aumenta a segurança das redes protegidas ao impedir que um navegador da Web envie comandos incorporados em solicitações de FTP.Após você habilitar a opção **strict** em uma interface, a inspeção de FTP passará a impor este comportamento.Um comando de FTP deverá ser confirmado para que o Security Appliance permita um novo comando.O Security Appliance descarta conexões que enviam comandos incorporados.Os comandos **227** e **PORT** são verificados para garantir que eles não fazem parte de strings de erro.**aviso:** O uso da opção *restrita* pôde causar a falha dos clientes de FTP que não são restritamente complacentes com FTP RFC. Consulte Uso da Opção strict para obter mais informações sobre o uso da opção **strict**.

Exemplo de configuração

Nome de dispositivo 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)#
```

Configuração da Inspeção do Protocolo FTP em Uma Porta TCP Não Padrão

Você pode configurar a inspeção do protocolo FTP para portas TCP não padrão usando estas linhas de configuração (substitua XXXX pelo número da nova porta):

```
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
```

Configuração da Inspeção Básica de Aplicativos de TFTP

Por padrão, a configuração inclui uma política que corresponde a todo o tráfego de inspeção de aplicativos padrão e aplica a inspeção ao tráfego em todas as interfaces (uma política global). O tráfego de inspeção de aplicativos padrão inclui o tráfego para as portas padrão para cada protocolo. É possível aplicar somente uma política global. Assim, se desejar alterar a política global, por exemplo, para aplicar inspeção a portas não padrão ou adicionar inspeções que não são habilitadas por padrão, você deverá editar a política padrão ou desabilitá-la e aplicar uma nova política. Para obter uma lista de todas as portas padrão, consulte Política de Inspeção Padrão.

1. Execute o comando **policy-map global_policy**.`ASAwAIP-CLI(config)#`**`policy-map global_policy`**
2. Execute o comando **class inspection_default**.`ASAwAIP-CLI(config-pmap)#`**`class inspection_default`**
3. Execute o comando **inspect TFTP**.`ASAwAIP-CLI(config-pmap-c)#`**`inspect TFTP`**

Exemplo de configuração

Nome de dispositivo 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)#
```

Verificar

Para garantir que a configuração tenha sido implementada com êxito, use o comando **show service-policy** e limite a saída somente à inspeção de FTP usando o comando **show service-policy inspect ftp**.

Troubleshooting

Problema: A sintaxe na configuração não trabalha e o erro de inspeção do mapa de classe é recebido

A sintaxe apresentada na seção de configuração não funciona e você recebe um erro semelhante a:

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

Solução

Esta configuração depende das inspeções padrão estarem presentes na configuração. Se não estiverem, recrie-as com os seguintes comandos:

1. **inspection_default do mapa de classepadrão-inspeção-tráfego do fósforo**
2. **policy-map type inspect dns preset_dns_map parametersmessage-length maximum 512**
3. **policy-map global_policyinspection_default da classeinspect dns preset_dns_mapinspect ftp inspect h323 h225inspecione os ras h323inspecione o rshinspecione o rtspinspecione o esmtpinspecione o sqlnetinspecione magroinspecione o sunrpcinspecione o xdmcpinspecione o sorvoinspecione o NetBIOSinspecione tftp**
4. **service-policy global_policy global**

aviso: Se as inspeçãos do padrão foram removidas previamente para resolver o outro problema, essa edição pôde retornar quando as inspeçãos do padrão re-são permitidas. Você ou o seu administrador devem saber se as inspeções padrão foram previamente removidas como uma etapa de troubleshooting.

Incapaz de executar FTP (FTP sobre o SSL) através do ASA

O FTP com TLS/SSL (SFTP/FTP) não é apoiado através da ferramenta de segurança. A conexão de FTP não é cifrada, tão lá é nenhuma maneira que o Firewall pode decifrar o pacote. Refira o PIX/ASA: Ferramenta de segurança FAQ para mais informação.

Informações Relacionadas

- Ferramentas de segurança adaptáveis do 5500 Series ASA
- Referência de comandos do dispositivo do Cisco Security
- Ferramenta de segurança da série PIX 500
- Recomendações de Segurança da Cisco e observações
- Suporte Técnico e Documentação - Cisco Systems