Evitar/que obstrui no IPS para o exemplo da configuração de roteador ASA/PIX/IOS

Índice

Introdução

Este documento descreve como configurar evitar em um IOS Router PIX/ASA/Cisco com a ajuda do ips Cisco. O ARCO, o aplicativo de obstrução no sensor, começa e blocos das paradas no Roteadores, no Cisco 5000 RS e nos Catalyst 6500 Series Switch, nos Firewall PIX, no FWSM, e no ASA. O ARCO emite um bloco ou evitar-lo ao dispositivo gerenciado para o endereço IP de Um ou Mais Servidores Cisco ICM NT malicioso. O ARCO envia o mesmo bloco a todos os dispositivos que o sensor controla. Se um sensor da obstrução mestra é configurado, o bloco está enviado a e emitido deste dispositivo. O ARC monitora o tempo para o bloco e remove o bloco quando o tempo expira.

Quando você usa IPS 5.1, o cuidado especial deve ser tomado quando evitar aos Firewall no modo de contexto múltiplo como nenhuma informação de VLAN é enviado com o pedido evitar.

Nota: Obstruir não é apoiada no contexto admin de um contexto múltiplo FWSM.

Há três tipos de blocos:

- Bloco do host — Obstrui todo o tráfego de um endereço IP de Um ou Mais Servidores Cisco ICM NT dado.
- Bloco da conexão — Os blocos traficam de um endereço IP de origem dado a um endereço IP de Um ou Mais Servidores Cisco ICM NT e a uma porta do destino do destino fornecido.Os blocos da conexão múltipla do mesmo endereço IP de origem a um endereço IP de destino diferente ou à porta do destino comutam automaticamente o bloco de um bloco da conexão a

um bloco do host.**Nota:** Os blocos da conexão não são apoiados por ferramentas de segurança. Blocos do host do apoio das ferramentas de segurança somente com informação de porta e protocolo opcional.
- Bloco da rede — Obstrui todo o tráfego de uma rede dada.Você pode iniciar blocos do host e da conexão manualmente ou automaticamente quando uma assinatura é provocada. Você pode somente iniciar blocos da rede manualmente.

Para blocos automáticos, você deve escolher o host do bloco de pedido ou a conexão do bloco de pedido como a ação do evento para assinaturas particular, de modo que SensorApp envie um pedido do bloco FORMAR ARCOS quando a assinatura é provocada. Uma vez que o ARCO recebe o pedido do bloco de SensorApp, atualiza as configurações de dispositivo para obstruir o host ou a conexão. Refira a atribuição de ações às assinaturas, pagine 5-22 para obter mais informações sobre do procedimento para adicionar as ações do host do bloco de pedido ou do evento de conexão do bloco de pedido à assinatura. Refira configurar a ação do evento cancela, paginam 7-15 para obter mais informações sobre do procedimento para a configuração de cancela que adiciona as ações do host do bloco de pedido ou do evento de conexão do bloco de pedido aos alarmes de avaliações de risco específicas.

Em roteadores Cisco e em Catalyst 6500 Series Switch, o ARCO cria blocos aplicando ACL ou VACL. Os ACL e os VACL aplicam filtros às relações, que inclui o sentido, e aos VLAN, respectivamente tráfego do permit or deny. O PIX Firewall, o FWSM, e o ASA não usam ACL ou VACL. O acessório **evita** e **nenhum comando shun** é usado.

Esta informação é exigida para a configuração do ARCO:

- Usuário de login - identificação, se o dispositivo é configurado com AAA
- Senha de login
- Permita a senha, que não é precisada se o usuário tem permitir privilégios
- Relações a ser controladas, por exemplo, ethernet0, vlan100
- Alguma informação que existente ACL ou VACL você quiser aplicado no início (PRE-bloco ACL ou VACL) ou fim (Cargo-bloco ACL ou VACL) do ACL ou do VACL que é criado. Isto não se aplica a um PIX Firewall, a um FWSM, ou a um ASA porque não usam ACL ou VACL para obstruir.
- Se você usa o telnet ou o SSH para se comunicar com o dispositivo
- Endereços IP de Um ou Mais Servidores Cisco ICM NT (host ou escala dos anfitriões) que você nunca quer obstruído
- Quanto tempo você quer os blocos durar

Pré-requisitos

Requisitos

Antes que você configure o ARCO para obstruir ou avalie a limitação, você deve terminar estas tarefas:

- Analise sua topologia de rede para compreender que dispositivos devem ser obstruídos por que o sensor, e que endereça deve nunca ser obstruído.
- Recolha os nomes de usuário, senhas do dispositivo, permita senhas, e os tipos de conexões (telnet ou SSH) precisaram de entrar a cada dispositivo.
- Conheça os nomes da relação nos dispositivos.

- Conheça os nomes do PRE-bloco ACL ou VACL e o Cargo-bloco ACL ou VACL se necessário.
- Compreenda que relações devem e não devem ser obstruídas e em que sentido (em ou para fora).

Componentes Utilizados

A informação neste documento é baseada no Sistema de prevenção de intrusões da Cisco 5.1 e mais atrasado.

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.

Nota: À revelia, o ARCO é configurado para um limite de 250 entradas de bloco. Refira dispositivos do apoio para obter mais informações sobre da lista de dispositivos de bloqueio apoiados pelo ARCO.

Convenções

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

Informações de Apoio

Use o painel de propriedades de obstrução a fim configurar as configurações básicas exigidas para permitir a obstrução e avaliar a limitação.

O ARCO controla a obstrução e avalia a limitação de ações em dispositivos gerenciado.

Você deve ajustar seu sensor a fim identificar os anfitriões e as redes que devem nunca ser obstruídos. É possível para o tráfego de um dispositivo confiável atear fogo a uma assinatura. Se esta assinatura é configurada para obstruir o atacante, o tráfego de rede legítimo pode ser afetado. O endereço IP de Um ou Mais Servidores Cisco ICM NT do dispositivo pode ser alistado nunca na lista da obstrução a fim impedir esta encenação.

Um netmask especificado em uma entrada de bloco é aplicado nunca nunca ao endereço de bloco. Se nenhum netmask é especificado, uma máscara de /32 do padrão é aplicada.

Nota: À revelia, o sensor não está permitido para emitir um bloco para seu próprio endereço IP de Um ou Mais Servidores Cisco ICM NT enquanto este interfere com a comunicação entre o sensor e o dispositivo de bloqueio. Mas, esta opção é configurável pelo usuário.

Uma vez que o ARCO é configurado para controlar um dispositivo de bloqueio, o dispositivo de bloqueio evita e os ACL/VACL que são usados obstruindo não devem ser alterados manualmente. Isto pode causar um rompimento do serviço do ARCO e pode conduzir aos blocos futuros que não estão sendo emitidos.

Nota: À revelia, somente obstruir é apoiada em dispositivos IOS Cisco. Você pode cancelar o

padrão de obstrução se você escolhe a taxa que limita ou que obstrui mais a limitação da taxa.

A fim emitir ou alterar blocos, o usuário IPS deve ter o papel do administrador ou do operador.

Configurar o sensor para controlar roteadores Cisco

Esta seção descreve como configurar o sensor para controlar roteadores Cisco. Contém estes assuntos:

- Configurar perfis de usuário
- Roteadores e ACL
- Configurar roteadores Cisco usando o CLI

Configurar perfis de usuário

O sensor controla os outros dispositivos com o comando do *profile_name dos* **perfis de usuário** a fim estabelecer perfis de usuário. Os perfis de usuário contêm o userid, senha, e permitem a informação de senha. Por exemplo, o Roteadores que todos compartilham das mesmos senhas e nomes de usuário pode estar sob um perfil de usuário.

Nota: Você **deve** criar um perfil de usuário antes que você configure o dispositivo de bloqueio.

Termine estas etapas a fim estabelecer perfis de usuário:

1. Entre ao CLI com uma conta que tenha privilégios do administrado.
2. Entre no modo de acesso de rede.`sensor#`**`configure terminal`** `sensor(config)#`**`service network-access`** `sensor(config-net)#`
3. Crie o nome do perfil de usuário.`sensor(config-net)#`**`user-profiles`** *`PROFILE1`*
4. Datilografe o username para esse perfil de usuário.`sensor(config-net-use)#`**`username`** *`username`*
5. Especifique a senha para o usuário.`sensor(config-net-use)# password Enter password[]: ******** Re-enter password ********`
6. Especifique a senha da possibilidade para o usuário.`sensor(config-net-use)# enable-password Enter enable-password[]: ******** Re-enter enable-password ********`
7. Verifique os ajustes.`sensor(config-net-use)#show settings profile-name: PROFILE1 ---------- ---------- enable-password: <hidden> password: <hidden> username: jsmith default: ---------- sensor(config-net-use)#`
8. Retire o submode do acesso de rede.`sensor(config-net-use)#exit sensor(config-net)#exit Apply Changes:?[yes]:`
9. A imprensa **entra** a fim aplicar as mudanças ou entrá-las não para rejeitá-las.

Roteadores e ACL

Quando o ARCO é configurado com um dispositivo de bloqueio que use ACL, os ACL são compostos desta maneira:

1. Uma linha da licença com o endereço IP de Um ou Mais Servidores Cisco ICM NT do sensor ou, se especificado, o endereço NAT do sensor**Nota:** Se você permite o sensor ser obstruído, esta linha não aparece no ACL.
2. PRE-bloco ACL (se especificado)Este ACL deve já existir no dispositivo.**Nota:** O ARCO lê as linhas no ACL PRE-configurado e copia estas linhas ao começo do bloco ACL.

3. Alguns blocos ativos
4. Qualquer um: Licença IP algum algum ACL/do Cargo-bloco- Cargo-**bloco ACL** (se especificado)Este ACL deve já existir no dispositivo.**Nota:** O ARCO lê as linhas no ACL e copia estas linhas ao fim do ACL.**Nota:** Certifique-se que a última linha no ACL é a licença IP todo o algum se você quer todos os pacotes ímpares ser permitido.- **licença IP algum algum** (não usado se um Cargo-bloco o ACL é especificado)

Nota: Os ACL que o ARCO faz deve nunca ser alterado por você ou algum outro sistema. Estes ACL são provisórios e os ACL novos são criados constantemente pelo sensor. As únicas alterações que você pode fazer são ao PRE e ao Cargo-bloco ACL.

Se você precisa de alterar o PRE-bloco ou o Cargo-bloco ACL, termine estas etapas:

1. Desabilite a obstrução no sensor.
2. Faça as mudanças à configuração do dispositivo.
3. Reenable que obstrui no sensor.

Quando obstruir reenabled, o sensor lê a configuração de dispositivo nova.

Nota: Um único sensor pode controlar dispositivos múltiplos, mas os sensores múltiplos não podem controlar um dispositivo único. No caso em que os blocos emitidos dos sensores múltiplos forem significados para um único dispositivo de bloqueio, um sensor da obstrução mestra deve ser incorporado no projeto. Um sensor de obstrução mestre recebe a obstrução de pedidos dos sensores múltiplos e emite todos os pedidos de obstrução ao dispositivo de bloqueio.

Você cria e salvar o PRE-bloco e o Cargo-bloco ACL em sua configuração de roteador. Estes ACL devem ser o IP extendido ACL, nomeado ou numerado. Veja sua documentação de roteador para obter mais informações sobre de como criar ACL.

Nota: O PRE-bloco e o Cargo-bloco ACL não se aplicam para avaliar a limitação.

Os ACL são invertidos avaliado e a ação do primeiro-fósforo é tomada. O PRE-bloco ACL pode conter uma licença que tome a precedência sobre uma negação que resultasse de um bloco.

O Cargo-bloco ACL é usado para esclarecer todas as circunstâncias não seguradas pelo PRE-bloco ACL ou por blocos. Se você tem um ACL existente na relação e no sentido que os blocos estão emitidos, esse ACL pode ser usado como o Cargo-bloco ACL. Se você não tem um Cargo-bloco ACL, as inserções do sensor permitem o IP algum no fim do ACL novo.

Quando o sensor começa acima, lê os índices dos dois ACL. Cria um terceiro ACL com estas entradas:

- Uma linha da licença para o endereço IP de Um ou Mais Servidores Cisco ICM NT do sensor
- Cópias de todas as linhas de configuração do PRE-bloco ACL
- Uma linha da negação para cada endereço que é obstruído pelo sensor
- Cópias de todas as linhas de configuração do Cargo-bloco ACL

O sensor aplicam o ACL novo à relação e o sentido que você designa.

Nota: Quando o bloco novo ACL é aplicado a uma relação do roteador, em uma direção específica, substitui todo o ACL de preexistência nessa relação nesse sentido.

Configurar roteadores Cisco usando o CLI

Termine estas etapas a fim configurar um sensor para controlar um roteador Cisco executar a obstrução e avaliar a limitação:

1. Entre ao CLI com uma conta que tenha privilégios do administrado.
2. Incorpore o submode do acesso de rede.`sensor#**configure terminal** sensor(config)#**service network-access** sensor(config-net)#`
3. Especifique o endereço IP de Um ou Mais Servidores Cisco ICM NT para o roteador controlado pelo ARCO.`sensor(config-net)#**router-devices** *ip_address*`
4. Dê entrada com o nome do dispositivo lógico que você criou quando você configurou o perfil de usuário.`sensor(config-net-rou)#**profile-name** *user_profile_name*` O ARCO aceita qualquer coisa que você incorpora. Não verifica para ver se o perfil de usuário existe.
5. Especifique o método usado para alcançar o sensor.`sensor(config-net-rou)# **communication {telnet | ssh-des | ssh-3des}**` Se não especificado, o SSH 3DES é usado.**Nota:** Se você usa o DES ou o 3DES, você deve usar o **comando ip_address da chave Host do ssh** a fim aceitar a chave SSH do dispositivo.
6. Especifique o endereço do sensor NAT.`sensor(config-net-rou)#**nat-address** *nat_address*` **Nota:** Isto muda o endereço IP de Um ou Mais Servidores Cisco ICM NT na primeira linha do ACL do endereço do sensor ao endereço NAT. O endereço NAT é o endereço do sensor, cargo-NAT, traduzido por um dispositivo intermediário, situado entre o sensor e o dispositivo de bloqueio.
7. Especifique se o roteador executa a obstrução, avalie a limitação, ou ambos.**Nota:** O padrão está obstruindo. Você não tem que configurar capacidades da resposta se você quer o roteador executar a obstrução somente.Taxa que limita somente`sensor(config-net-rou)#**response-capabilities rate-limit**` Obstruindo e avalie a limitação`sensor(config-net-rou)#**response-capabilities block|rate-limit**`
8. Especifique o nome e o sentido da relação.`sensor(config-net-rou)#**block-interfaces** *interface_name* **{in | out}**` **Nota:** O nome da relação deve ser uma abreviatura que o roteador reconheça quando usado após o **comando interface**.
9. (Opcional) adicionar o nome PRE-ACL (que obstrui somente).`sensor(config-net-rou-blo)#**pre-acl-name** *pre_acl_name*`
10. (Opcional) adicionar o nome cargo-ACL (que obstrui somente).`sensor(config-net-rou-blo)#**post-acl-name** *post_acl_name*`
11. Verifique os ajustes.`sensor(config-net-rou-blo)#**exit** sensor(config-net-rou)#**show settings**`
    ```
    ip-address: 10.89.127.97 ---------------------------------------------- communication:
    ssh-3des default: ssh-3des nat-address: 19.89.149.219 default: 0.0.0.0 profile-name:
    PROFILE1 block-interfaces (min: 0, max: 100, current: 1) ---------------------------------
    -------------- interface-name: GigabitEthernet0/1 direction: in -------------------------
    --------------------- pre-acl-name: <defaulted> post-acl-name: <defaulted> ---------------
    ------------------------------- ---------------------------------------------- response-
    capabilities: block|rate-limit default: block ------------------------------------------
    --- sensor(config-net-rou)#
    ```
12. Retire o submode do acesso de rede.`sensor(config-net-rou)#**exit** sensor(config-net)#**exit** sensor(config)#**exit** Apply Changes:?[yes]:`
13. A imprensa **entra** a fim aplicar as mudanças ou entrá-las **não** para rejeitá-las.

Configurar o sensor para controlar Firewall de Cisco

Termine estas etapas a fim configurar o sensor para controlar Firewall de Cisco:

1. Entre ao CLI com uma conta que tenha privilégios do administrado.
2. Incorpore o submode do acesso de rede.`sensor#**configure terminal** sensor(config)#**service**`

network-access sensor(config-net)#

3. Especifique o endereço IP de Um ou Mais Servidores Cisco ICM NT para o Firewall controlado pelo ARCO.`sensor(config-net)#`**`firewall-devices`** *`ip_address`*
4. Dê entrada com o nome do perfil de usuário que você criou quando você configurou o perfil de usuário.`sensor(config-net-fir)#`**`profile-name`** *`user_profile_name`* O ARCO aceita qualquer coisa que você datilografa. Não verifica para ver se o dispositivo lógico existe.
5. Especifique o método usado para alcançar o sensor.`sensor(config-net-fir)#`**`communication {telnet | ssh-des | ssh-3des}`** Se não especificado, o SSH 3DES é usado.**Nota:** Se você usa o DES ou o 3DES, você deve usar o **comando ip_address da chave Host do ssh** a fim aceitar a chave ou o ARCO não pode conectar ao dispositivo.
6. Especifique o endereço do sensor NAT.`sensor(config-net-fir)#`**`nat-address`** *`nat_address`* **Nota:** Isto muda o endereço IP de Um ou Mais Servidores Cisco ICM NT na primeira linha do ACL do endereço IP de Um ou Mais Servidores Cisco ICM NT do sensor ao endereço NAT. O endereço NAT é o endereço do sensor, cargo-NAT, traduzido por um dispositivo intermediário, situado entre o sensor e o dispositivo de bloqueio.
7. Retire o submode do acesso de rede.`sensor(config-net-fir)#`**`exit`** `sensor(config-net)#`**`exit`** `sensor(config)#`**`exit`** `Apply Changes:?[yes]:`
8. A imprensa **entra** a fim aplicar as mudanças ou entrá-las **nenhum** a fim rejeitá-las.

O bloco com EVITA no PIX/ASA

Emitir o **comando shun** obstrui conexões de um host de ataque. Os pacotes que combinam os valores no comando estão deixados cair e registrados até que a função de obstrução esteja removida. **Evitar** é aplicado apesar de se uma conexão com o endereço de host especificado é atualmente ativo.

Se você especifica o endereço de destino, portas de origem e de destino, e o protocolo, você reduz evitar às conexões que combinam aqueles parâmetros.

Você pode somente ter um **comando shun** para cada endereço IP de origem.

Porque o **comando shun** é usado obstruir dinamicamente ataques, não é indicado na configuração da ferramenta de segurança.

Sempre que uma relação é removida, tudo evita que é anexado a essa relação é removido igualmente.

Este exemplo mostra que o host de ofensa (10.1.1.27) faz uma conexão com a vítima (10.2.2.89) ao TCP. A conexão na tabela de conexão da ferramenta de segurança lê como segue:

```
TCP outside:10.1.1.27/555 inside:10.2.2.89/666
```

A fim obstruir conexões de um host de ataque, use o **comando shun no** modo de exec privilegiado. Aplique o **comando shun** com estas opções:

```
hostname#shun 10.1.1.27 10.2.2.89 555 666 tcp
```

O comando suprime da conexão da tabela de conexão da ferramenta de segurança e igualmente impede pacotes de 10.1.1.27:555 a 10.2.2.89:666 (TCP) de atravessar a ferramenta de segurança.

Informações Relacionadas

- Configurando o sensor para controlar Catalyst 6500 Series Switch e Cisco 7600 Series Router
- Configurar o controlador da resposta do ataque para obstruir e avalia a limitação usando IDM 7.0
- Suporte Técnico e Documentação - Cisco Systems