ASA/PIX 7.x e mais tarde: Abrandando os ataques de rede

Índice

Introdução

Este documento descreve como reduzir os vários ataques à rede, tais como os Recusa de Serviços (DoS), usando o Cisco Security Appliance (ASA/PIX).

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

A informação neste documento é baseada na ferramenta de segurança adaptável do Cisco 5500 Series (ASA) essa versão de software 7.0 das corridas 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.

Produtos Relacionados

Este documento pode igualmente ser usado com Cisco 500 Series PIX que executa a versão de software 7.0 e mais atrasado.

Convenções

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

Proteção contra ataques SYN

Como você abranda os ataques do sincronizar/começo do Transmission Control Protocol (TCP) (SYN) no ASA/PIX?

Ataque SYN TCP

O ataque SYN TCP é um tipo de ataque DoS em que um remetente transmite um volume de conexões que não possa ser terminado. Isso faz com que as filas de conexões sejam preenchidas e, conseqüentemente, o atendimento aos usuários TCP legítimos seja recusado.

Quando uma conexão de TCP normal começa, um host de destino recebe um pacote SYN de um host de origem e envia para trás um sincronizar reconhece (SYN ACK). O host de destino deve então ouvir um ACK do SYN ACK antes que a conexão esteja estabelecida. Isto é referido como o cumprimento de três vias TCP.

Enquanto aguarda o ACK para o SYN ACK, uma fila de conexão de tamanho finito no host de destino mantém o controle das conexões aguardando conclusão. Esta fila esvazia tipicamente rapidamente porque o ACK é esperado chegar alguns milissegundos após o SYN ACK.

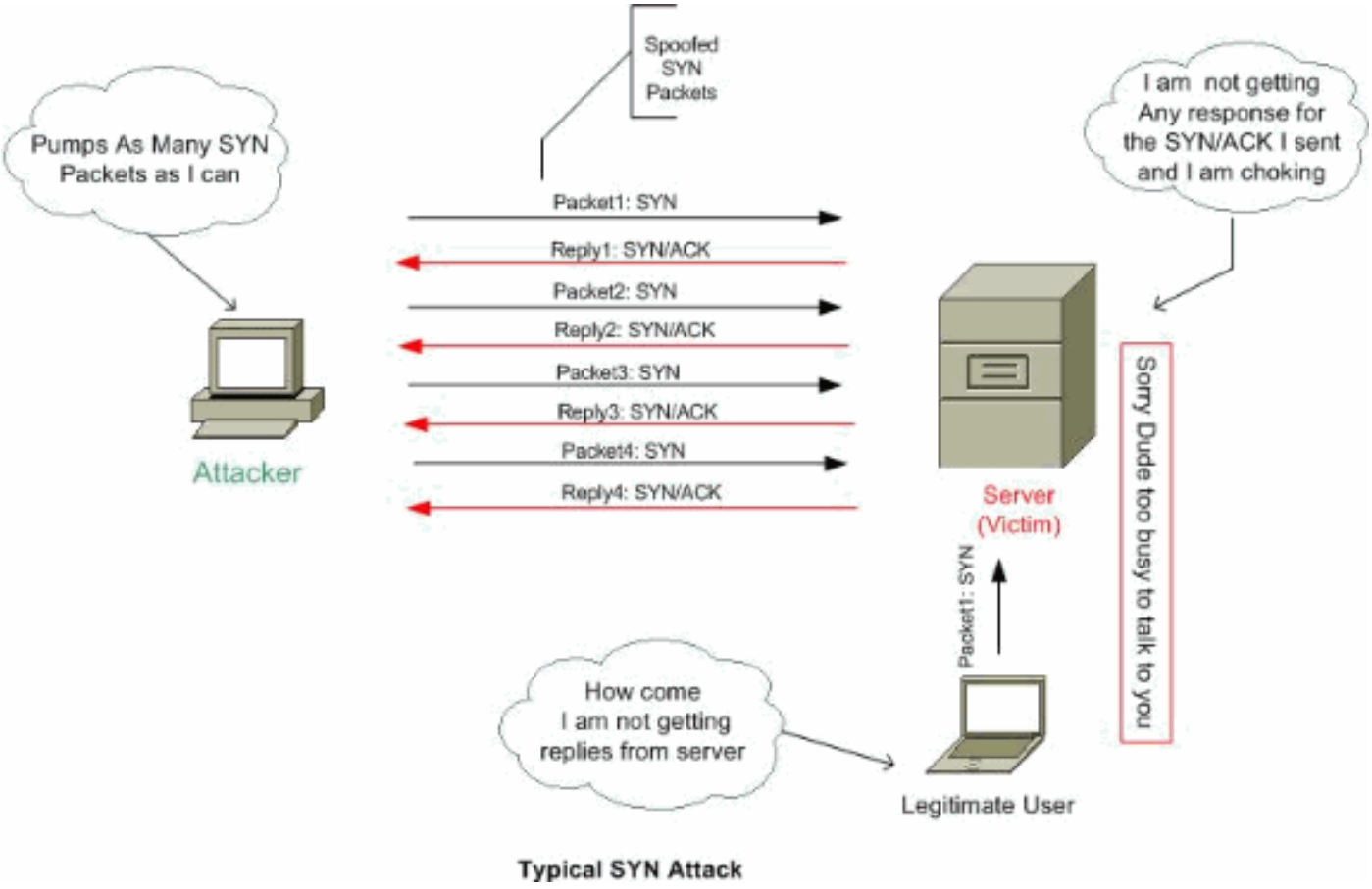
O ataque SYN em TCP explora esse projeto ao fazer um host de origem de ataque gerar pacotes SYN no TCP com endereços de origem aleatórios em direção ao host de uma vítima. O host de destino da vítima envia um SYN ACK de volta ao endereço de origem aleatório e adiciona uma entrada à fila de conexão. Porque o SYN ACK é destinado para um host incorreto ou inexistente, o último o “cumprimento de três vias” é terminado parte de nunca e a entrada permanece na fila de conexão até que um temporizador expire, tipicamente para aproximadamente um minuto. Gerando pacotes SYN de TCP falsos dos endereços IP de Um ou Mais Servidores Cisco ICM NT aleatórios em uma taxa rápida, é possível encher acima a fila de conexão e negar serviços TCP (tais como o email, a transferência de arquivo, ou o WWW) aos usuários legítimos.

Não há nenhuma maneira fácil seguir o autor do ataque porque o endereço IP de Um ou Mais Servidores Cisco ICM NT da fonte é forjado.

As manifestações externas do problema incluem a incapacidade receber o email, a incapacidade aceitar conexões ao WWW ou aos serviços de FTP, ou as um grande número conexões de TCP em seu host no estado SYN_RCVD.

Refira defesas contra ataques de inundação de SYN TCP para obter mais informações sobre dos

ataques SYN TCP.



Typical SYN Attack

Mitigação

Esta seção descreve como abrandar os ataques SYN ajustando o máximo TCP e conexões do User Datagram Protocol (UDP), conexões embriônica máximas, timeouts de conexão, e como desabilitar o randomization da sequência TCP.

Se o limite da conexão embriônica é alcançado, a seguir a ferramenta de segurança responde a cada pacote SYN enviado ao server com um SYN+ACK, e não passa o pacote SYN ao servidor interno. Se o dispositivo externo responde com um pacote de ACK, a seguir a ferramenta de segurança sabe que é um pedido válido (e não parte de um ataque SYN potencial). A ferramenta de segurança então estabelece uma conexão com o server e junta-se às conexões junto. Se a ferramenta de segurança não recebe de volta um ACK do server, cronometra agressivelmente para fora essa conexão embriônica.

Cada conexão de TCP tem o número de sequência inicial dois (ISN): um gerado pelo cliente e um gerado pelo server. A ferramenta de segurança randomizes o ISN do TCP SYN que passa no de entrada e em direções externas.

Randomizing o ISN do host protegido impede que um atacante prever o ISN seguinte para uma nova conexão e sequestre potencialmente a sessão nova.

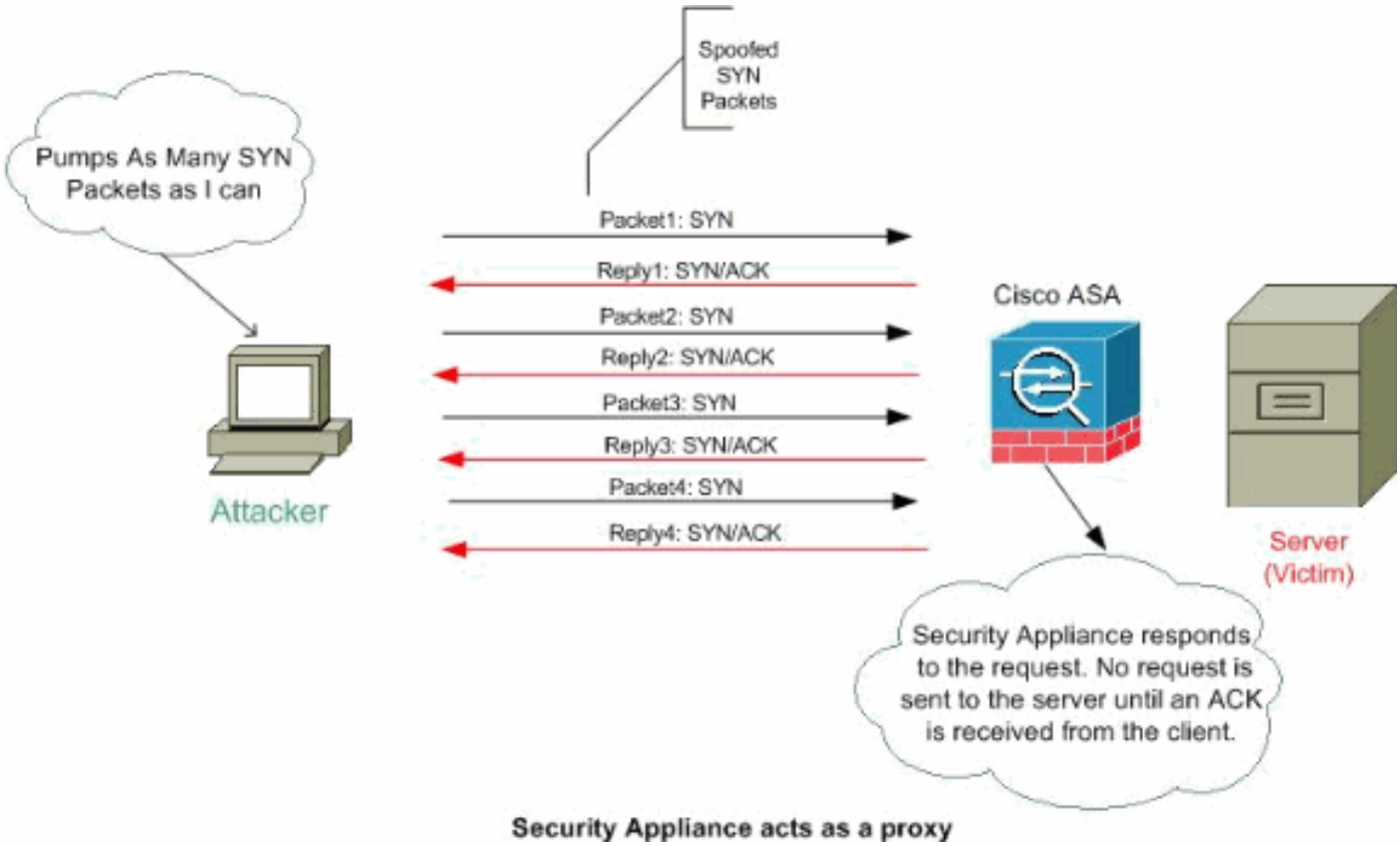
O randomization do número de sequência inicial TCP pode ser desabilitado se for necessário. Por exemplo:

- Se uma outra em-linha Firewall igualmente randomizing os números de sequência iniciais, não há nenhuma necessidade para que ambos os Firewall executem esta ação, mesmo que

esta ação não afete o tráfego.

- Se você usa o multi-salto do BGP externo (eBGP) através da ferramenta de segurança, e os pares do eBGP estão usando o MD5, o randomization quebra a soma de verificação MD5.
- Você usa um dispositivo do Wide Area Application Services (WAAS) que exija a ferramenta de segurança não randomize os números de sequência de conexões.

Nota: Você pode igualmente configurar conexões máxima, conexões embriônica máximas, e de sequência TCP randomization na configuração de NAT. Se você configura estes ajustes para o mesmo tráfego usando ambos os métodos, a seguir a ferramenta de segurança usa o limite mais baixo. Para o randomization da sequência TCP, se é desabilitada usando um ou outro método, a seguir a ferramenta de segurança desabilita o randomization da sequência TCP.



Security Appliance acts as a proxy

Termine estas etapas a fim ajustar limites da conexão:

1. A fim identificar o tráfego, adicionar um mapa da classe usando o **comando class-map** de acordo com a utilização da estrutura de política modular.
2. A fim adicionar ou editar um **mapa de política** que ajusta as ações para tomar com o tráfego do mapa da classe, incorpore este comando:`hostname(config)#`**`policy-map name`**
3. A fim identificar o mapa da classe (de etapa 1) a que você quer atribuir uma ação, incorpore este comando:`hostname(config-pmap)#`**`class class_map_name`**
4. A fim ajustar as conexões máxima (TCP e UDP), as conexões embriônica máximas, por-cliente-embrionário-MAX, por-cliente-MAX ou se desabilitar o randomization da sequência TCP, incorporam este comando:`hostname(config-pmap-c)#`**`set connection`** `{[`**`conn-max`** `number] [`**`embryonic-conn-max`** `number] [`**`per-client-embryonic-max`** `number] [`**`per-client-max`** `number][`**`random-sequence-number`** `{`**`enable`** `|` **`disable`**`}}` Onde o número é um inteiro entre 0 e 65535. O padrão é 0, que não significa nenhum limite em conexões.Você pode inscrever este comando all em uma linha (em alguma ordem), ou você pode incorporar cada atributo enquanto um comando separado. O comando é combinado em uma linha na configuração running.

5. A fim ajustar o intervalo para conexões, as conexões embriônica (metade-abertas) e as conexões entreabertas, incorporam este comando:`hostname(config-pmap-c)#`**`set connection`** `{[`**`embryonic`** `hh[:mm[:ss]]] [`**`half-closed`** `hh[:mm[:ss]]] [`**`tcp`** `hh[:mm[:ss]]]}` Onde HH **embrionário** [: milímetro [: os ss] são um momento entre 0:0:5 e 1192:59:59. O padrão é 0:0:30. Você pode igualmente ajustar este valor a 0, que significa que a conexão nunca cronometra para fora.O HH **entreaberto** [: milímetro [: ss] e **tcp** HH [: milímetro [: os valores ss] são um momento entre 0:5:0 e 1192:59:59. O padrão para **entreaberto** é 0:10:0 e o padrão para o **tcp** é 1:0:0. Você pode igualmente ajustar estes valores a 0, que significa que a conexão nunca cronometra para fora.Você pode inscrever este comando all em uma linha (em alguma ordem), ou você pode incorporar cada atributo enquanto um comando separado. O comando é combinado em uma linha na configuração running.**Conexão (Metade-aberta) embrionária** — Uma conexão embriônica é um pedido de conexão de TCP que não termine o aperto de mão necessário entre a fonte e o destino.**Conexão entreaberta** — A conexão entreaberta é quando a conexão é fechada somente em um sentido enviando o FIN. Contudo, a sessão de TCP é mantida ainda pelo par.**Por-cliente-embrionário-MAX** — O número máximo de conexões embriônica simultâneas permitidas pelo cliente, entre 0 e 65535. O padrão é 0, que permite conexões ilimitadas.**Por-cliente-MAX** — O número máximo de conexões simultâneas permitidas pelo cliente, entre 0 e 65535. O padrão é 0, que permite conexões ilimitadas.
6. A fim ativar o mapa de política em umas ou várias relações, incorpore este comando:`hostname(config)#`**`service-policy policymap_name`** *`{global | interface interface_name}`* Onde **global** aplica o mapa de política a todas as relações, e a **relação** aplica a política a uma relação. Somente uma política global é permitida. Você pode cancelar a política global em uma relação aplicando uma política de serviços a essa relação. Você pode somente aplicar um mapa de política a cada relação.

Exemplo:

```
ciscoasa(config)#class-map tcp_syn ciscoasa(config-cmap)#match port tcp eq 80 ciscoasa(config-
cmap)#exit ciscoasa(config)#policy-map tcpmap ciscoasa(config-pmap)#class tcp_syn
ciscoasa(config-pmap-c)#set connection conn-max 100 ciscoasa(config-pmap-c)#set connection
embryonic-conn-max 200 ciscoasa(config-pmap-c)#set connection per-client-embryonic-max 10
ciscoasa(config-pmap-c)#set connection per-client-max 5 ciscoasa(config-pmap-c)#set connection
random-sequence-number enable ciscoasa(config-pmap-c)#set connection timeout embryonic 0:0:45
ciscoasa(config-pmap-c)#set connection timeout half-closed 0:25:0 ciscoasa(config-pmap-c)#set
connection timeout tcp 2:0:0 ciscoasa(config-pmap-c)#exit ciscoasa(config-pmap)#exit
ciscoasa(config)#service-policy tcpmap global
```

Nota: A fim verificar o número total de sessões entreabertas para todo o host particular, use este comando:

```
ASA-5510-8x# show local-host all Interface dmz: 0 active, 0 maximum active, 0 denied Interface
management: 0 active, 0 maximum active, 0 denied Interface xx: 0 active, 0 maximum active, 0
denied Interface inside: 7 active, 18 maximum active, 0 denied local host: <10.78.167.69>, TCP
flow count/limit = 2/unlimited TCP embryonic count to host = 0 TCP intercept watermark =
unlimited UDP flow count/limit = 0/unlimited
```

Nota: A linha, `contagem embrionária TCP a hospedar`, indica o número de sessões entreabertas.

Proteção contra ataques da falsificação de IP

Pode o PIX/ASA obstruir ataques falsos IP?

Falsificação de IP

A fim aceder, os intrusos criam pacotes com os endereços IP de origem falsificado. Isto explora os aplicativos que usam a autenticação baseada em endereços IP de Um ou Mais Servidores Cisco ICM NT e condu-los ao usuário não autorizado e possivelmente ao acesso raiz no sistema alvo. Os exemplos são os serviços rsh e de rlogin.

Épossível aos pacotes de rota com os Firewall do roteador de filtragem se não são configurados para filtrar os pacotes recebidos cujo o endereço de origem está no domínio local. É importante notar que o ataque descrito é possível mesmo se nenhum pacote de resposta pode alcançar o atacante.

Os exemplos de configurações que são potencialmente vulneráveis incluem:

- Firewall do proxy onde os aplicativos do proxy usam o endereço IP de origem para a autenticação
- Roteadores às redes externas que apoiam interfaces internas múltiplas
- Roteadores com duas relações que apoiam o sub-rede na rede interna

Mitigação

Protetores do Unicast Reverse Path Forwarding (uRPF) contra a falsificação de IP (um pacote usa um endereço IP de origem incorreto para obscurecer seu origem verdadeira) assegurando-se de que todos os pacotes tenham um endereço IP de origem que combine a interface de origem correta de acordo com a tabela de roteamento.

Normalmente, a ferramenta de segurança olha somente o endereço de destino ao determinar onde enviar o pacote. O unicast RPF instrui a ferramenta de segurança para olhar igualmente o endereço de origem. Eis porque é chamado **encaminhamento de caminho reverso**. Para todo o tráfego que você quiser permitir através da ferramenta de segurança, a tabela de roteamento da ferramenta de segurança deve incluir uma rota de volta ao endereço de origem. Veja o RFC 2267 para mais informação.

Nota: `:- %PIX-1-106021: Negue a verificação do caminho reverso do protocolo do src_addr ao dest_addr no` mensagem de registro do `int_name da relação` pode ser visto quando a verificação do caminho reverso é permitida. Desabilite a verificação do caminho reverso com **nenhum IP verificam o** comando da **relação do caminho reverso (nome da relação)** a fim resolver esta edição:

```
no ip verify reverse-path interface (interface name)
```

Para o tráfego exterior, por exemplo, a ferramenta de segurança pode usar a rota padrão para satisfazer a proteção do unicast RPF. Se o tráfego entra de uma interface externa, e o endereço de origem não está sabido à tabela de roteamento, a ferramenta de segurança usa a rota padrão para identificar corretamente a interface externa como a interface de origem.

Se o tráfego incorpora a interface externa de um endereço que esteja sabido à tabela de roteamento, mas é associado com a interface interna, então a ferramenta de segurança deixa cair o pacote. Similarmente, se o tráfego incorpora a interface interna de um endereço de origem desconhecida, a ferramenta de segurança deixa cair o pacote porque a rota de harmonização (a rota padrão) indica a interface externa.

O unicast RPF é executado como mostrado:

- Os pacotes ICMP não têm nenhuma sessão, assim que cada pacote é verificado.

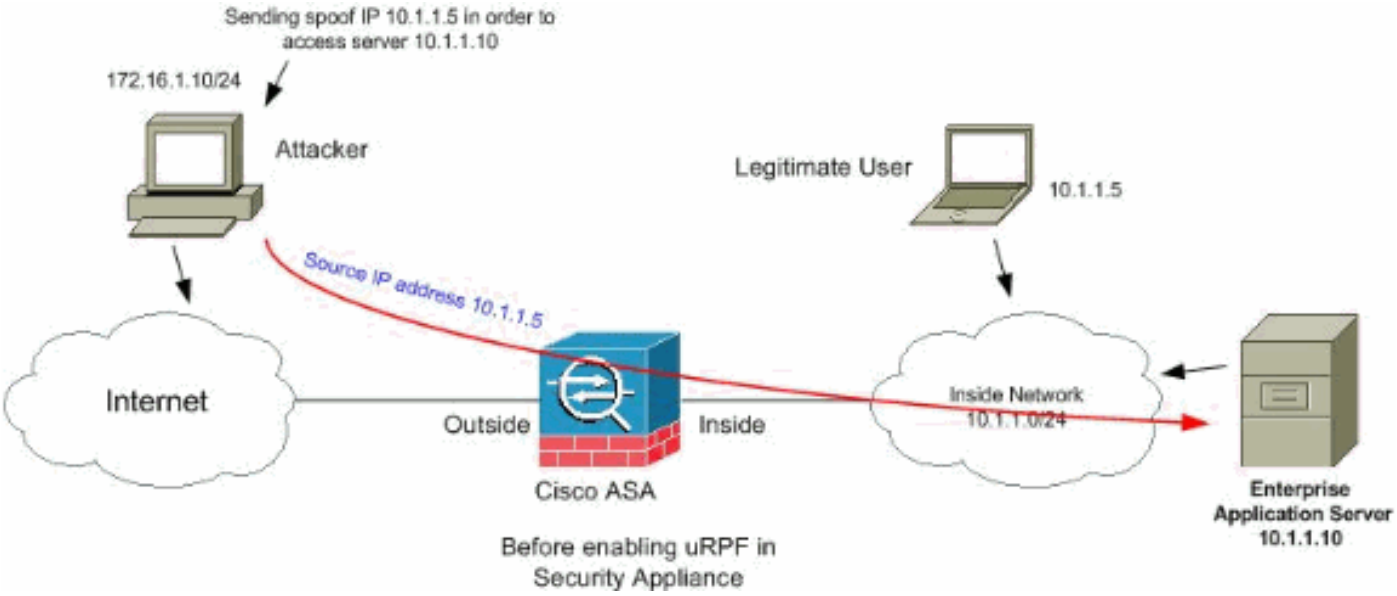
- O UDP e o TCP têm sessões, assim que o pacote inicial exige uma consulta reversa da rota. Os pacotes subsequente que chegam durante a sessão são verificados usando um estado existente mantido como parte da sessão. os pacotes NON-iniciais são verificados para assegurar-se de que cheguem na mesma relação usada pelo pacote inicial.

A fim permitir o unicast RPF, incorpore este comando:

```
hostname(config)#ip verify reverse-path interface interface_name
```

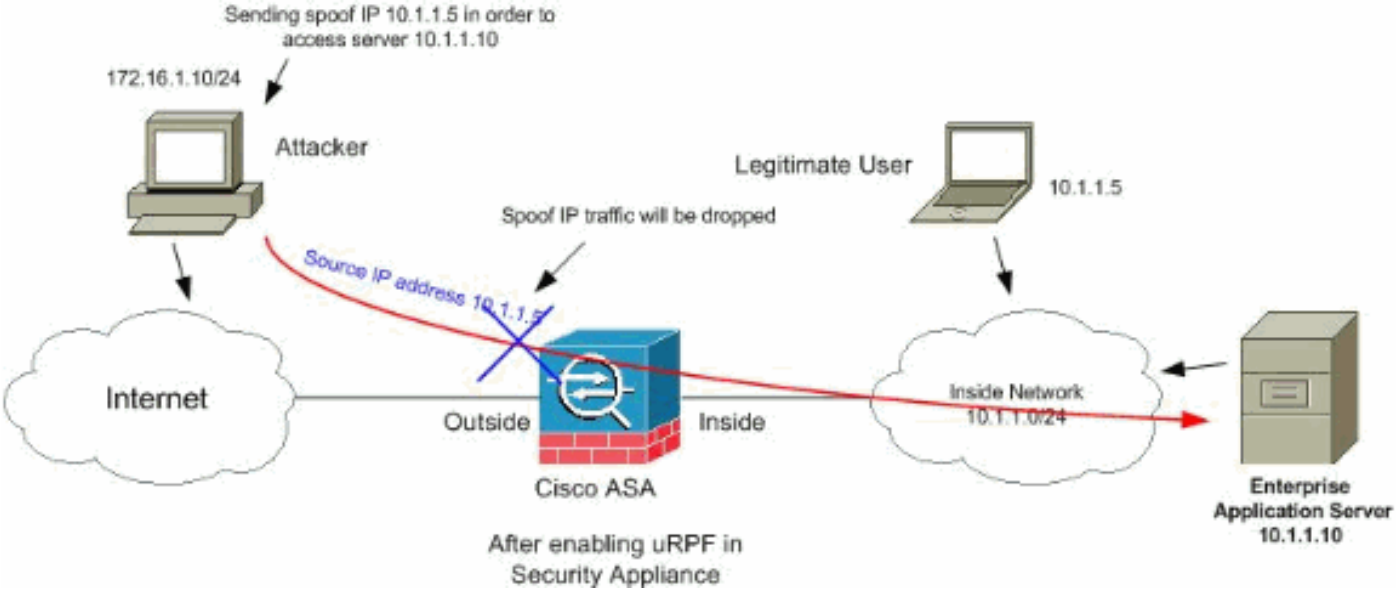
Exemplo:

Como mostrado esta figura, o atacante PC origina um pedido ao server de aplicativo 10.1.1.10 enviando um pacote com um endereço IP de origem forjado 10.1.1.5/24, e o server envia um pacote ao endereço IP real 10.1.1.5/24 em resposta ao pedido. Este tipo de pacote ilegal atacará o server de aplicativo e o usuário legítimo na rede interna.



O unicast RPF pode impedir os ataques baseados na falsificação de endereço de origem. Você precisa de configurar como mostrado o uRPF na interface externa do ASA aqui:

```
ciscoasa(config)#ip verify reverse-path interface outside
```



Identificação da falsificação usando mensagens do syslog

A ferramenta de segurança mantém-se receber Mensagens de Erro do Syslog como mostrado. Isto indica que os ataques potenciais usando pacotes falsificado ou aquele puderam provocar devido ao roteamento assimétrico.

1. **%PIX|ASA-2-106001: Inbound TCP connection denied from IP_address/port to IP_address/port flags tcp_flags on interface interface_name** **Explicação**Esta é uma mensagem relacionada à conexão. Esta mensagem ocorre quando uma tentativa de conectar a um endereço interno é negada pela política de segurança que está definida para o tipo do tráfego especificado. Os valores possíveis dos *tcp_flags* correspondem às bandeiras no cabeçalho de TCP que estou presente quando a conexão foi negada. Por exemplo, um pacote de TCP chegou para qual nenhum estado de conexão existe na ferramenta de segurança, e foi deixada cair. *Os tcp_flags n*este pacote são FIN e ACK.*Os tcp_flags* são como segue:ACK — O número de reconhecimento foi recebido.FIN — Os dados foram enviados.PSH — O receptor passou dados ao aplicativo.RST — A conexão foi restaurada.SYN — Os números de sequência foram sincronizados para começar uma conexão.URG — O ponteiro urgente era válido declarado.Há muitas razões para que a tradução estática falhe no PIX/ASA. Mas, um motivo comum é se a relação da zona desmilitarizada (DMZ) está configurada com o mesmo nível de segurança (0) que a interface externa.A fim resolver esta edição, atribua um nível de segurança diferente a todas as relaçõesRefira configurar parâmetros da relação para mais informação.Este Mensagem de Erro igualmente aparece se um dispositivo externo envia um pacote de identificação ao cliente interno, que está deixado cair pelo PIX Firewall. Refira os problemas de desempenho de PIX causados pelo Protocolo IDENT para mais informação
2. **%PIX|ASA-2-106007: Deny inbound UDP from outside_address/outside_port to inside_address/inside_port due to DNS {Response|Query}** **Explicação**Esta é uma mensagem relacionada à conexão. Esta mensagem é indicada se a conexão especificada falha devido a um **comando deny de partida**. A variável do protocolo pode ser ICMP, TCP, ou UDP.**Ação recomendada:** Use o **comando outbound da mostra** verificar listas externas.
3. `%PIX|ASA-3-106014: Deny inbound icmp src interface_name: IP_address dst interface_name: IP_address (type dec, code dec)`**Explicação**A ferramenta de segurança negou todo o acesso do pacote do ICMP de entrada. À revelia, todos os pacotes ICMP são negados o acesso a menos que permitidos especificamente.
4. `%PIX|ASA-2-106016: Deny IP spoof from (IP_address) to IP_address on interface interface_name.`**Explicação**Esta mensagem é gerada quando um pacote chega na relação da ferramenta de segurança que tem um endereço IP de destino de 0.0.0.0 e um endereço MAC de destino da relação da ferramenta de segurança. Além, esta mensagem é gerada quando a ferramenta de segurança rejeitou um pacote com um endereço de origem inválido, que possa incluir um do seguinte ou algum outro endereço inválido:Rede do laço de retorno (127.0.0.0)Transmissão (limitado, rede-dirigido, sub-rede-dirigido, e todo-sub-rede-dirigido)O host de destino (land.c)A fim aumentar mais a detecção do pacote do spoof, use o **comando icmp** configurar a ferramenta de segurança para rejeitar pacotes com os endereços de origem que pertencem à rede interna. Isto é porque o **comando access-list** foi suplicado e é garantido já não para trabalhar corretamente.**Ação recomendada:** Determine se um usuário externo está tentando comprometer a rede protegida. Verifique para ver se há clientes desconfigurados.
5. `%PIX|ASA-2-106017: Deny IP due to Land Attack from IP_address to IP_address`**Explicação**A ferramenta de segurança recebeu um pacote com o endereço IP de origem igual ao destino IP, e a porta do destino igual à porta de origem. Esta mensagem indica um pacote falsificado que seja projetado atacar sistemas. Este ataque é referido como

um ataque da terra.**Ação recomendada:** Se esta mensagem persiste, um ataque pôde ser em andamento. O pacote não fornece bastante informação para determinar onde o ataque origina.

6. `%PIX|ASA-1-106021: Deny protocol reverse path check from source_address to dest_address on interface interface_name`**Explicação**Um ataque é em andamento. Alguém está tentando ao spoof um endereço IP de Um ou Mais Servidores Cisco ICM NT em uma conexão de entrada. Unicast RPF, igualmente conhecido como a consulta reversa da rota, detectada um pacote que não tenha um endereço de origem representado por uma rota e suponha que é parte de um ataque em sua ferramenta de segurança.Esta mensagem aparece quando você permitiu o unicast RPF com o **IP verifica o** comando do **caminho reverso**. Esta característica trabalha nos pacotes entrados a uma relação. Se é configurada na parte externa, a seguir a ferramenta de segurança verifica os pacotes que chegam da parte externa.A ferramenta de segurança olha acima uma rota baseada no endereço de origem. Se uma entrada não é encontrada e uma rota não está definida, a seguir este mensagem de Log de sistema aparece e a conexão é deixada cair.Se há uma rota, a ferramenta de segurança verifica que relação corresponde. Se o pacote chegou em uma outra relação, é ou um spoof ou há um ambiente do roteamento assimétrico que tenha mais de um trajeto a um destino. A ferramenta de segurança não apoia o roteamento assimétrico.Se a ferramenta de segurança é configurada em uma interface interna, verifica instruções de comando ou RASGO da rota estática. Se o endereço de origem não é encontrado, a seguir um usuário interno é falsificação seu endereço.**Ação recomendada:** Mesmo que um ataque seja em andamento, se esta característica é permitida, nenhuma ação de usuário está exigida. A ferramenta de segurança repele o ataque.**Nota:** O comando da **gota asp da mostra** mostra os pacotes ou as conexões deixados cair pelo trajeto acelerado da Segurança (asp), que pôde o ajudar a pesquisar defeitos um problema. Igualmente indica quando a última vez onde os contadores de queda asp foram cancelados. Use o comando RPF-**violado gota asp da mostra em** que o contador é incrementado quando o **IP verifica que o caminho reverso** está configurado em uma relação e a ferramenta de segurança recebe um pacote para que a consulta da rota do IP da fonte não rendeu a mesma relação que essa em que o pacote foi recebido.`ciscoasa#`**`show asp drop frame rpf-violated`** `Reverse-path verify failed 2` **Nota: Recomendação:** Siga a fonte de tráfego baseada no IP da fonte impresso neste mensagem de sistema seguinte, e investigue porque está enviando o tráfego falsificado.**Nota: Mensagens de Log de sistema:** 106021
7. `%PIX|ASA-1-106022: Deny protocol connection spoof from source_address to dest_address on interface interface_name`**Explicação**Um pacote que combina uma conexão chega em uma relação diferente da relação onde a conexão começou.Por exemplo, se um usuário começa uma conexão na interface interna, mas a ferramenta de segurança detecta a mesma conexão chegar em uma relação do perímetro, a ferramenta de segurança tem mais de um trajeto a um destino. Isto é sabido como o roteamento assimétrico e não apoiado na ferramenta de segurança.Um atacante igualmente pôde tentar adicionar pacotes de uma conexão a outra como uma maneira de quebrar na ferramenta de segurança. Em qualquer dos casos, a ferramenta de segurança indica esta mensagem e deixa cair a conexão.**Ação da recomendação:** Esta mensagem aparece quando o **IP verifica que** comando do **caminho reverso** não está configurado. Certifique-se do roteamento não esteja assimétrico.
8. `%PIX|ASA-4-106023: Deny protocol src [interface_name:source_address/source_port] dst interface_name:dest_address/dest_port [type {string}, code {code}] by access_group acl_ID`**Explicação**Um pacote IP foi negado pelo ACL. Este exibições de

mensagem mesmo se você não tem a opção do **log** permitida para um ACL.**Ação da recomendação:** Se as mensagens persistem do mesmo endereço de origem, as mensagens puderam indicar uma tentativa da pé-impressão ou da porta-exploração. Contacte os administradores do host remoto.

9. `%PIX|ASA-3-210011: Connection limit exceeded cnt/limit for dir packet from sip/sport to dip/dport on interface if_name.`
10. `%ASA-4-419002: Received duplicate TCP SYN from in_interface:src_address/src_port to out_interface:dest_address/dest_port with different initial sequence number.` **Explicação**Este mensagem de Log de sistema indica que aquele estabelecer uma nova conexão através do dispositivo de firewall conduzirá a exceder pelo menos uma da máxima configurada dos limites da conexão. O mensagem de Log de sistema aplica ambos para a conexão limita configurado usando um comando static, ou àqueles configurados usando a estrutura de política modular de Cisco. A nova conexão não será permitida através do dispositivo de firewall até que uma das conexões existentes esteja rasgado para baixo, trazendo desse modo a contagem da conexão atual abaixo da máxima configurada.*cnt* — Contagem da conexão atual*limite* — Limite configurado da conexão*dir* — Direção de tráfego, de entrada ou de partida*sorvo* — Endereço IP de origem*esporte* — Porta de origem*mergulho* — Endereço IP de destino*dport* — Porta do destino*if_name* — Nome da relação em que a unidade do tráfego é recebida, preliminar ou secundário.**Ação da recomendação:** Porque os limites da conexão são configurados para um bom motivo, este mensagem de Log de sistema poderia indicar um ataque possível DoS, neste caso a fonte do tráfego poderia provavelmente ser um endereço IP de Um ou Mais Servidores Cisco ICM NT falsificado. Se o endereço IP de origem não é totalmente aleatório, identificar a fonte e obstrui-la que usa uma lista de acesso puderam ajudar. Em outros casos, obter farejadores de rastreamento e analisar a fonte do tráfego ajudariam em isolar o tráfego não desejado do tráfego legitimado.

Característica básica da detecção da ameaça em ASA 8.x

O dispositivo ASA/PIX do Cisco Security apoia a característica chamada detecção da ameaça da versão de software 8.0 e mais atrasado. Usando a detecção básica da ameaça, a ferramenta de segurança monitora a taxa de pacotes descartado e de eventos de segurança devido a estas razões:

- Recusa por Listas de acesso
- Formato de pacote de informação ruim (tal como o inválido-IP-encabeçamento ou o inválido-TCP-HDR-comprimento)
- Limites da conexão excedidos (ambos os limites sistema-largos do recurso, e grupo de limites na configuração)
- Ataque DoS detectado (como uma falha do SPI inválido, da verificação do firewall stateful)
- Verificações básicas do Firewall falhadas (esta opção é uma taxa combinada que inclua todas as quedas de pacote de informação Firewall-relacionadas nesta lista bulleted. Não inclui gotas NON-Firewall-relacionadas tais como a sobrecarga da relação, os pacotes falhados na inspeção de aplicativo, e o ataque da exploração detectado.)
- Pacotes ICMP suspeitos detectados
- Inspeção de aplicativo falhada pacotes
- Sobrecarga da relação
- Ataque de varredura detectado (esta opção monitora ataques da exploração; por exemplo, o primeiro pacote de TCP não é um pacote SYN, ou a conexão de TCP falhou o aperto de mão

da 3-maneira. A detecção completa da ameaça da exploração (refira configurar a detecção da ameaça da exploração para mais informação) toma esta informação de taxa do ataque da exploração e atua nela classificando anfitriões como atacantes e automaticamente evitando os, por exemplo.)
- Detecção incompleta da sessão tal como o ataque SYN TCP detectado ou nenhum ataque da sessão de UDP dos dados detectado.

Quando a ferramenta de segurança detecta uma ameaça, envia imediatamente um mensagem de Log de sistema (730100).

A detecção básica da ameaça afeta o desempenho somente quando há umas gotas ou umas ameaças potenciais. Mesmo nesta encenação, o impacto no desempenho é insignificante.

O comando rate da ameaça-detecção da mostra está usado a fim identificar ataques potenciais quando você é registrado na ferramenta de segurança.

```
ciscoasa#show threat-detection rate Average(eps) Current(eps) Trigger Total events 10-min ACL
drop: 0 0 0 16 1-hour ACL drop: 0 0 0 112 1-hour SYN attck: 5 0 2 21438 10-min Scanning: 0 0 29
193 1-hour Scanning: 106 0 10 384776 1-hour Bad pkts: 76 0 2 274690 10-min Firewall: 0 0 3 22 1-
hour Firewall: 76 0 2 274844 10-min DoS attck: 0 0 0 6 1-hour DoS attck: 0 0 0 42 10-min
Interface: 0 0 0 204 1-hour Interface: 88 0 0 318225
```

Refira configurar a seção básica da detecção da ameaça do manual de configuração ASA 8.0 para obter mais informações sobre da divisória da configuração.

Mensagem do syslog 733100

Mensagem de erro:

```
%ASA-4-733100: Object drop rate rate_ID exceeded. Current burst rate is rate_val per second, max
configured rate is rate_val; Current average rate is rate_val per second, max configured rate is
rate_val; Cumulative total count is total_cnt
```

O objeto especificado no mensagem de Log de sistema excedeu a taxa especificada do ponto inicial da explosão ou a taxa média do ponto inicial. O objeto pode ser atividade da gota de um host, da porta TCP/UDP, do protocolo IP, ou das várias gotas devido aos ataques potenciais. Indica que o sistema está sob o ataque potencial.

Nota: Estes Mensagens de Erro com definição são aplicáveis somente a ASA 8.0 e mais atrasado.

1. Objeto — O general ou o origem específica de uma contagem da taxa da gota, que pudesse incluir estes:Guarda-fogoPacotes ruinsLimite de taxaAttck DoSGota ACLLimite conexãoAttk ICMPVarreduraAttck SYNInspecioneInterface
2. rate_ID — A taxa configurada que está sendo excedida. A maioria de objetos podem ser configurados com até três taxas diferentes para intervalos diferentes.
3. rate_val — Um valor de taxa particular.
4. total_cnt — O contagem total desde que o objeto foi criado ou cancelado.

Estes três exemplos mostram como estas variáveis ocorrem:

- Para uma gota da relação devido a uma limitação CPU ou de barramento:`%ASA-4-733100: [Interface] drop rate 1 exceeded. Current burst rate is 1 per second, max configured rate is 8000; Current average rate is 2030 per second, max configured rate is 2000; Cumulative total count is 3930654`

- Para uma gota da exploração devido aos ataques potenciais:`ASA-4-733100: [Scanning] drop rate-1 exceeded. Current burst rate is 10 per second_ max configured rate is 10; Current average rate is 245 per second_ max configured rate is 5; Cumulative total count is 147409 (35 instances received)`
- Para pacotes devido ruim aos ataques potenciais:`%ASA-4-733100: [Bad pkts] drop rate 1 exceeded. Current burst rate is 0 per second, max configured rate is 400; Current average rate is 760 per second, max configured rate is 100; Cumulative total count is 1938933`

Ação recomendada:

Execute estas etapas de acordo com o tipo de objeto especificado que aparece na mensagem:

1. Se o objeto no mensagem do syslog é um destes:Guarda-fogoPacotes ruinsLimite de taxaAtaque DoSGota ACLLimite conexãoAttk ICMPVarreduraAttck SYNInspecioneInterfaceVerifique se a taxa da gota seja aceitável para o ambiente running.
2. Ajuste a taxa do ponto inicial da gota particular a um valor apropriado executando o *comando xxx da* **taxa da ameaça-detecção**, onde *xxx* são um destes:ACL-gotaruim-pacote-gotaCONN-limite-gotados-gotaFW-gotaICMP-gotainspecionar-gotarelação-gotaexploração-ameaçaataque SYN
3. Se o objeto no mensagem do syslog é uma porta TCP ou UDP, um protocolo IP, ou uma gota do host, verificação se a taxa da gota é aceitável para o ambiente running.
4. Ajuste a taxa do ponto inicial da gota particular a um valor apropriado executando o comando da ruim-pacote-**gota da taxa da ameaça-detecção**. Refira a seção básica configurando da detecção da ameaça do manual de configuração ASA 8.0 para mais informação.

Nota: Se você não quer a taxa da gota exceda o aviso para aparecer, você pode desabilitá-lo não executando **nenhum** comando da básico-**ameaça da ameaça-detecção**.

Informações Relacionadas

- Página de suporte adaptável das ferramentas de segurança do Cisco 5500 Series
- Página do suporte de PIX do Cisco 500 Series
- Defesas contra ataques de inundação de SYN TCP
- Cisco aplicou o boletim da mitigação: Identificando e exploração do abrandamento da vulnerabilidade de negação de serviço no módulo content switching
- Cisco aplicou o boletim da mitigação: Identificando e exploração do abrandamento das múltiplas vulnerabilidades em Cisco PIX e em dispositivos ASA e em módulo de serviços de firewall
- Falsificação de IP
- Suporte Técnico e Documentação - Cisco Systems