Cisco guia para endurecer o Firewall de Cisco ASA

Índice

Introdução

Este documento contém a informação para ajudá-lo a fixar dispositivos de Cisco ASA, que aumenta a segurança total de sua rede. Este documento é estruturado em 4 seções

Endurecimento do plano de gerenciamento - Isto aplica a todo o Management/To relativo ASA o tráfego da caixa como SNMP, SSH etc.
Fixando os comandos config através de que nós podemos parar de povoar as senhas etc. para a configuração running etc.
Registrar e monitorar - Isto aplica-se a quaisquer ajustes relativos a entrar o ASA.
Com o tráfego - Isto aplica-se ao tráfego que atravessa o ASA.

A cobertura dos recursos de segurança neste documento fornece frequentemente bastante detalhes para que você configure a característica. Contudo, nos casos onde não faz, a característica é explicada de tal maneira que você pode avaliar se a atenção adicional à característica está exigida. Sempre que possível e apropriado, este documento contém as recomendações que, se executadas, ajudam a fixar a rede.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

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

- Cisco ASA5500-X 9.4(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.

Produtos Relacionados

Esta configuração pode igualmente ser usada com versão de software 9.x da ferramenta de segurança do 5500-X Series de Cisco ASA.

Convenções

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

Fixe operações

As operações de rede seguras são um assunto substancial. Embora a maioria deste documento seja devotado à configuração segura de um dispositivo de Cisco ASA, as configurações apenas não fixam completamente uma rede. Os procedimentos operacionais no uso na rede contribuem tanto quanto à segurança quanto a configuração dos dispositivos subjacentes.

Estes assuntos contêm as recomendações operacionais que você é recomendado executar. Estes assuntos destacam áreas crítica específicas das operações de rede e não são detalhados.

Monitore Recomendações de Segurança da Cisco e respostas

A equipe da resposta de incidentes de segurança de produto Cisco (PSIRT) cria e mantém as publicações, referidas geralmente como informativos psirt, para edições relacionadas à segurança nos produtos da Cisco. O método usado para uma comunicação de edições menos severas é a resposta do Cisco Security. As Recomendações de Segurança e as respostas estão disponíveis no PSIRT.

A informação adicional sobre estes veículos de uma comunicação está disponível na política da vulnerabilidade do Cisco Security.

A fim manter uma rede segura, você precisa de estar ciente das Recomendações de Segurança da Cisco e das respostas que foram liberadas. Você precisa de ter o conhecimento de uma vulnerabilidade antes que a ameaça que possa levantar a uma rede possa ser avaliada. Refira a triagem do risco para anúncios da vulnerabilidade de segurança para o auxílio a este processo de avaliação.

Entrega de Autenticação, Autorização e Relatório

A estrutura do Authentication, Authorization, and Accounting (AAA) é vital fixar dispositivos de rede. A estrutura AAA fornece a autenticação das sessões de gerenciamento e pode igualmente limitar usuários a comandos específico, definidos pelos administradores e aos comandos all do registro inscritos por todos os usuários. Veja a seção do autenticação, autorização e relatório deste documento para obter mais informações sobre de como leverage o AAA.

Centralize a coleção e a monitoração do registro

A fim ganhar o conhecimento sobre a existência, emergindo, e os eventos históricos relacionaram-se aos incidentes de segurança, sua organização deve ter uma estratégia unificada para o logging de evento e a correlação. Esta estratégia deve entregar o registo de todos os dispositivos de rede e usar capacidades pré-embaladas e customizáveis da correlação.

Depois que o registo centralizado é executado, você deve desenvolver uma aproximação estruturada para registrar o seguimento da análise e do incidente. Baseado nas necessidades de sua organização, esta aproximação pode variar de uma revisão diligente simples dos dados de registro a análise baseado em regras avançada.

Use protocolos seguros quando possível

Muitos protocolos são usados a fim levar dados de gerenciamento de redes sensíveis. Você deve usar protocolos seguros sempre que possível. Uma escolha segura do protocolo inclui o uso do SSH em vez do telnet de modo que os dados de autenticação e a informação de gerenciamento sejam cifrados. Além, você deve usar protocolos de transferência de arquivo seguros quando você copia dados de configuração. Um exemplo é o uso do protocolo da cópia segura (SCP) no lugar do FTP ou do TFTP.

Ganhe a visibilidade do tráfego com NetFlow

O NetFlow permite-o de monitorar fluxos de tráfego na rede. Pretendeu originalmente exportar a informação de tráfego para aplicativos de gerenciamento de rede, NetFlow pode igualmente ser usado a fim mostrar a informação de fluxo em um roteador. Esta capacidade permite que você considere que tráfego atravessa a rede no tempo real. Apesar da informação de fluxo ser exportada para um coletor remoto, é recomendado configurar dispositivos de rede para o NetFlow de modo que possa ser usado de forma reativa, se necessário.

Gerenciamento de configuração

O gerenciamento de configuração é um processo pelo qual as alterações de configuração são propostas, revistas, aprovadas, e distribuídas. Dentro do contexto de uma configuração de dispositivo de Cisco ASA, dois aspectos adicionais do gerenciamento de configuração são críticos: configuração de arquivo e segurança.

Você pode usar arquivos de configuração para rolar para trás as mudanças que são feitas aos dispositivos de rede. Em um contexto de segurança, os arquivos de configuração podem igualmente ser usados a fim determinar que alterações de segurança foram feitas e quando estas mudanças ocorreram. Conjuntamente com dados de registro AAA, esta informação pode ajudar no exame de segurança dos dispositivos de rede.

A configuração de um dispositivo de Cisco ASA contém muitos detalhes sensíveis. Os nomes de usuário, as senhas, e os índices de lista de controle de acesso são exemplos deste tipo de informação. O repositório que você usa a fim arquivar configurações de dispositivo de Cisco ASA precisa de ser fixado. O acesso incerto a esta informação pode minar a segurança da toda a rede.

Plano de gerenciamento

O plano de gerenciamento consiste nas funções que conseguem os objetivos da gestão da rede. Isto inclui as sessões de gerenciamento interativas que usam o SSH, assim como estatística-recolhem-no com SNMP ou Netflow. Quando você considera a segurança de um dispositivo de rede, é crítico que o plano de gerenciamento esteja protegido. Se um incidente de segurança pode minar as funções do plano de gerenciamento, pode ser impossível para você recuperar ou estabilizar a rede.

Endurecendo o plano de gerenciamento

O plano de gerenciamento é usado a fim alcançar, configurar, e controlar um dispositivo, assim como monitora suas operações e a rede em que é distribuído. O plano de gerenciamento é o plano que recebe e envia o tráfego para operações destas funções. Esta lista de protocolos é usada pelo plano de gerenciamento:

- Protocolo simples de gestão de rede
- Protocolo secure shell
- Protocolo de transferência de arquivo
- Protocolo trivial file transfer
- Protocolo da cópia segura
- TACACS+
- RADIUS
- Netflow
- Protocolo de tempo de rede
- Syslog
- ICMP
- SMB

Nota: Permitir TELNET não é recomendada porque é texto simples.

Gerenciamento de senha

Acesso do controle das senhas aos recursos ou aos dispositivos. Isto é realizado com a definição uma senha ou um segredo que sejam usados a fim autenticar pedidos. Quando um pedido é recebido para o acesso a um recurso ou a um dispositivo, o pedido está desafiado para a verificação da senha e da identidade, e o acesso pode ser concedido, negado, ou limitado baseado no resultado. Como um melhor prática da segurança, as senhas devem ser controladas com um TACACS+ ou um servidor de autenticação RADIUS. Contudo, note que uma senha localmente configurada para o acesso de privilegiado está precisada ainda no caso da falha do TACACS+ ou dos serviços de raio. Um dispositivo pode igualmente ter a outra informação de senha atual dentro de sua configuração, tal como uma chave NTP, a chave da série de comunidade SNMP, ou do protocolo de roteamento.

O ASA usa o message digest 5 (MD5) para o hashing da senha. Este algoritmo teve a revisão pública considerável e não é sabido para ser reversível. Contudo, o algoritmo é sujeito aos ataques do dicionário. Em um ataque do dicionário, um atacante tenta cada palavra em um dicionário ou a outra lista de senhas do candidato a fim de encontrar uma combinação. Conseqüentemente, os arquivos de configuração devem firmemente ser armazenados e somente compartilhado com os indivíduos confiados.

Permita o serviço HTTP

Para usar o ASDM, você precisa de permitir o servidor HTTPS, e permite conexões de HTTPS ao ASA. A ferramenta de segurança permite um máximo de exemplos simultâneos 5 ASDM pelo contexto, se disponível, com um máximo de 32 exemplos ASDM entre todos os contextos. Para configurar o uso do acesso ASDM:

```
http server enable <port>
```

Permita somente o IP que são precisadas na lista ACL. Permitir um acesso largo é uma errada pratica.

```
http 0.0.0.0 0.0.0.0 <interface>
```

Configurar o controle de acesso ASDM:

```
http <remote_ip_address> <remote_subnet_mask> <interface_name>
```

Começando com software release ASA 9.1(2),8.4(4.1), O ASA apoia agora as seguintes séries efêmeras da cifra de Diffie-Hellman (DHE) SSL.

DHE-AES128-SHA1
DHE-AES256-SHA1

Estas séries da cifra são especificadas no **RFC 3268**, Advanced Encryption Standard (AES) Ciphersuites para o Transport Layer Security (TLS).

Quando apoiado pelo cliente, DHE é a cifra preferida porque fornece o discrição perfeita adiante. Veja as seguintes limitações:

DHE não é apoiado em conexões do 3.0 SSL, assim que certifique-se permitir igualmente o TLS1.0 para o servidor SSL.

```
// Set server version ASA(config)# ssl server-version tlsv1 sslv3
// Set client version ASA(config) # ssl client-version any
```

Alguns aplicativos popular não apoiam DHE, assim que inclua pelo menos outro um método de criptografia SSL para assegurar-se de que uma série da cifra comum ao cliente SSL e ao server possa ser usada. Alguns clientes não podem apoiar DHE, incluindo AnyConnect 2.5 e 3.0, Cisco Secure Desktop, e internet explorer 9.0.

O ASA tem abaixo das cifras permitidas na ordem como abaixo à revelia.

```
ASA(config)#ssl encryption rc4-sha1 dhe-aes128-sha1 dhe-aes256-sha1 aes128-sha1 aes256-sha1
3des-sha1
```

versão de servidor SSL (padrão)

O ASA usa à revelia um certificado auto-assinado provisório que mude em cada repartição. Se você está procurando um único certificado, você pode seguir o link abaixo para gerar um certificado auto-assinado permanente.

Agora o startig da versão TLS 1.2 dos apoios ASA da versão de software 9.3.1for fixa a transmissão de mensagem para o ASDM, os sem clientes SSVPN, e o AnyConnect VPN. Os comandos seguintes foram introduzidos ou alteraram comandos: **versão de cliente SSL**, **versão**

de servidor SSL, **cifra SSL**, confiança-**ponto SSL**, DH-**grupo SSL**, **SSL da mostra**, **cifra SSL da mostra**, **mostra VPN-sessiondb**

```
ASA-1/act(config)# ssl server-version ?

configure mode commands/options:
  tlsv1    Enter this keyword to accept SSLv2 ClientHellos and negotiate TLSv1
           (or greater)
  tlsv1.1  Enter this keyword to accept SSLv2 ClientHellos and negotiate
           TLSv1.1 (or greater)
  tlsv1.2  Enter this keyword to accept SSLv2 ClientHellos and negotiate
           TLSv1.2 (or greater)
ASA-1/act(config)# ssl cipher ?

configure mode commands/options:
  default  Specify the set of ciphers for outbound connections
  dtlsv1   Specify the ciphers for DTLSv1 inbound connections
  tlsv1    Specify the ciphers for TLSv1 inbound connections
  tlsv1.1  Specify the ciphers for TLSv1.1 inbound connections
  tlsv1.2  Specify the ciphers for TLSv1.2 inbound connections
```

Permita o SSH

O ASA permite conexões de SSH ao ASA para propósitos do gerenciamento. O ASA permite um máximo das conexões de SSH 5 simultâneas pelo contexto, se disponível, com um máximo de 100 conexões divididas entre todos os contextos.

```
hostname <device_hostname>
domain-name <domain-name>
crypto key generate rsa modulus 2048
```

O tipo do par de chaves do padrão é chave geral. O tamanho do módulo do padrão é 1024. A quantidade de espaço NVRAM para armazenar pares de chaves varia segundo a plataforma ASA. Você pode alcançar um limite se você gerencie mais de 30 pares de chaves. As chaves 4096-bit RSA são apoiadas somente no ASA5580, nos 5585, ou nas Plataformas mais atrasadas.

Para remover os pares de chaves do tipo indicado (rsa ou dsa)

```
crypto key zeroize { rsa | dsa } [ label key-pair-label ] [ default ] [ noconfirm ]
```

Configurar o SSH para o acesso do dispositivo remoto:

```
ssh <remote_ip_address> <remote_subnet_mask> <interface_name>
```

Para restringir a versão do SSH aceitada pelo ASA, use o comando version do ssh no modo de configuração global. Para restringir o ASA para usar somente a versão 2 pode ser don wusing abaixo do comando.

```
ASA(config)#ssh version 2
```

Para trocar chaves usando o método das trocas de chave do grupo1 do Diffie-Hellman (DH) ou do grupo 14 DH, use o comando das trocas de chave do ssh no modo de configuração global. partir 9.1(2) do ASA apoia dh-group14-sha1 para o SSH

```
ASA(config)#ssh key-exchange dh-group14-sha1
```

Configurar o intervalo para sessões de login

```
// Configure Console timeout
ASA(config)#console timeout 10

// Configure Console timeout
```

```
ASA(config)#ssh timeout 10
```

Gerenciamento de senha

Acesso do controle das senhas aos recursos ou aos dispositivos. Isto é realizado com a definição uma senha ou um segredo que sejam usados a fim autenticar pedidos. Quando um pedido é recebido para o acesso a um recurso ou a um dispositivo, o pedido está desafiado para a verificação da senha e da identidade, e o acesso pode ser concedido, negado, ou limitado baseado no resultado. Como um melhor prática da segurança, as senhas devem ser controladas com um TACACS+ ou um servidor de autenticação RADIUS. Contudo, note que uma senha localmente configurada para o acesso de privilegiado está precisada ainda no caso da falha do TACACS+ ou dos serviços de raio. Um dispositivo pode igualmente ter a outra informação de senha atual dentro de sua configuração, tal como uma chave NTP, a chave da série de comunidade SNMP, ou do protocolo de roteamento.

Configurar o usuário local e a senha criptografada

```
username <local_username> password <local_password> encrypted
```

Configurar permitem a senha

```
enable password <enable_password> encrypted
```

Configurar a autenticação de AAA para o modo enable

```
ASA(config)#aaa authentication enable console LOCAL
```

Autenticação, autorização e contabilidade

A estrutura do Authentication, Authorization, and Accounting (AAA) é crítica a fim fixar o acesso interativo aos dispositivos de rede. A estrutura AAA fornece um ambiente altamente configurável que possa ser costurado baseie nas necessidades da rede.

Autenticação TACACS+

O TACACS+ é um protocolo de autenticação que o ASA possa usar para a autenticação de usuários do Gerenciamento contra um servidor AAA remoto. Estes usuários do Gerenciamento podem alcançar o dispositivo ASA através do SSH, do HTTPS, do telnet, ou do HTTP.

A autenticação TACACS+, ou mais geralmente a autenticação de AAA, fornecem a capacidade para usar o usuário individual esclarecem cada administrador de rede. Quando você não depende de uma única senha compartilhada, a Segurança da rede está melhorada e sua responsabilidade é reforçada.

O RAIO é um protocolo similar na finalidade ao TACACS+; contudo, cifra somente a senha enviada através da rede. Ao contrário, o TACACS+ cifra o payload de TCP inteiro, que inclui ambos o nome de usuário e senha. Por este motivo, o TACACS+ deve ser usado de preferência ao RADIUS quando o TACACS+ é suportado pelo servidor AAA. Refira a comparação de TACACS+ e RADIUS para uma comparação mais detalhada destes dois protocolos.

A autenticação TACACS+ pode ser permitida em um dispositivo de Cisco ASA com uma configuração similar a este exemplo:

```
aaa authentication serial console Tacacs
aaa authentication ssh console Tacacs
```

```
aaa authentication http console Tacacs
aaa authentication telnet console Tacacs
```

Assinatura e verificação da imagem ASA

Partir das imagens da versão de software 9.3.1 ASA é assinada agora usando uma assinatura digital. A assinatura digital é verificada depois que o ASA é carreg.

```
ASA-1/act(config)# verify flash:/asa941-smp-k8.bin
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!Done! Embedded Hash SHA-512:
0e707a0e45b1c7c5afa9ef4e802a273677a5e46f7e1d186292abe1154
c948a63c625463b74119194da029655487659490c2873506974cab78b66d6d9742ed73e Computed Hash SHA-512:
0e707a0e45b1c7c5afa9ef4e802a273677a5e46f7e1d186292abe1154
c948a63c625463b74119194da029655487659490c2873506974cab78b66d6d9742ed73e CCO Hash SHA-512:
1b6d41e893868aab9e06e78a9902b925227c82d8e31978ff2c412c18a
c99f49f70354715441385e0b96e4bd3e861d18fb30433d52e12b15b501fa790f36d0ea0 Signature Verified
ASA(config)# verify /signature running Requesting verify signature of the running image...
Starting image verification Hash Computation: 100% Done! Computed Hash SHA2:
2fbb0f62b5fbc61b081acfca76bddbb2 26ce7a5fb4b424e5e21636c6c8a7d665
1e688834203dfb7ffa6eaefc7fdf9d3d 1d0a063a20539baba72c2526ca37771c Get key records from key
storage: PrimaryASA, key_store_type: 6 Embedded Hash SHA2: 2fbb0f62b5fbc61b081acfca76bddbb2
26ce7a5fb4b424e5e21636c6c8a7d665 1e688834203dfb7ffa6eaefc7fdf9d3d
1d0a063a20539baba72c2526ca37771c Returned. rc: 0, status: 1 The digital signature of the running
image verified successfully

ASA-1/act(config)# show software authenticity running
Image type : Release
Signer Information
Common Name : abraxas
Organization Unit : ASAv
Organization Name : CiscoSystems
Certificate Serial Number : 550DBBD5
Hash Algorithm : SHA2 512
Signature Algorithm : 2048-bit RSA
Key Version : A
```

Configurar a zona de tempo

```
clock timezone GMT <hours offset>
```

Configurar o NTP

O protocolo Network Time Protocol (NTP) é um não serviço especialmente perigoso, mas todo o serviço unneeded pode representar um vetor do ataque. Se o NTP é usado, é importante configurar explicitamente um origem de tempo confiado e usar a autenticação apropriada. A hora exata e segura for exigida para finalidades syslog, como durante investigações judiciais dos ataques potenciais, assim como para a conectividade de VPN bem sucedida quando segundo certificados para a autenticação da fase 1.

- **Zona de hora (fuso horário) NTP** - Quando você configura o NTP, a zona de hora (fuso horário) precisa de ser configurada de modo que os timestamps possam exatamente ser correlacionados. Há geralmente duas aproximações para configurar a zona de hora (fuso horário) para dispositivos em uma rede com uma presença global. Um método é configurar todos os dispositivos de rede com o tempo universal coordenado (UTC) (previamente horário de Greenwich (GMT)). A outra aproximação é configurar dispositivos de rede com o fuso horário local.

```
ntp server ip_address [ key key_id ] [ source interface_name ] [ prefer ]
```

- **Autenticação de NTP** - Se você configura a autenticação de NTP, oferece a garantia que os mensagens de NTP estão trocados entre pares confiados NTP. Permita a autenticação usando o comando ntp authenticate, ajuste a chave confiada ID para este server. Se você permite a autenticação, o ASA comunica-se somente com um servidor de NTP se usa a chave confiada correta nos pacotes. Para permitir a autenticação com um servidor de NTP, use o comando ntp authenticate no modo de configuração global.

```
ASA(config)#ntp authenticate
```

Serviço do servidor DHCP (se não sendo usado)

```
clear configure dhcpd
no dhcpd enable <interface_name>
```

Nota: O ASA não apoia o CDP.

Lista de acesso do controle plano

As regras do controle de acesso para o tráfego de gerenciamento da à--caixa (definido por comandos como o HTTP, o ssh, ou o telnet) têm a precedência superior do que uma lista de acessos aplicada com a opção do controle plano. Consequentemente, tal tráfego de gerenciamento permitido será permitido entrar mesmo se negado explicitamente pela lista de acessos da à--caixa.

```
access-list <name> in interface <Interface_name> control-plane
```

Do ASA

Estão aqui os protocolos que podem ser usados para copiar/arquivos de transferência ao ASA.

Texto claro:

- FTP
- HTTP
- TFTP
- SMB

Fixe:

- HTTPS
- O SCP (cliente da cópia segura) que parte de 9.1(5), ASA apoia o SCP cliente para transferir arquivos a e de um server SCP.

Para o tráfego direto

Randomization do número de sequência TCP

Cada conexão de TCP tem dois ISN: um gerado pelo cliente e um gerado pelo server. O ASA 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 predecting 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 eBGP com o ASA, e os pares do eBGP estão usando o MD5. O Randomization quebra a soma de verificação MD5.
- Se nós usamos um dispositivo WAAS que exija o ASA não randomize os números de sequência de conexões.

Decréscimo TTL

Àrevelia, não decresce o TTL no cabeçalho IP devido a que ASA não aparece como um salto do roteador ao fazer Traceroute.

dnsguard

Reforça uma resposta de DNS pela pergunta. Pode ser permitida usando o comando no modo de configuração global.

```
ASA(config)#dns-guard
```

Configurar as verificações Chain da fragmentação do fragmento

Para fornecer o Gerenciamento adicional da fragmentação de pacote de informação e melhorar a compatibilidade com NFS, use o comando fragment no modo de configuração global.

```
fragment reassembly { full | virtual } { size | chain | timeout limit } [ interface ]
```

Configurar a inspeção do protocolo

Os motores da inspeção são exigidos para os serviços que encaixam a informação do endereçamento de IP no pacote de dados do usuário ou que os canais secundários abertos em portas dinamicamente atribuídas. Estes protocolos exigem o ASA fazer uma inspeção de pacote de informação profunda em vez de passar o pacote através do caminho rápido. Em consequência, os motores da inspeção podem afetar o throughput geral. Consulte por favor o guia da configuração ASA 9.4 para a informação detalhada na inspeção do protocolo de camada do aplicativo.

A inspeção no ASA pode ser utilização permitida abaixo do comando

```
policy-map <Policy-map_name>
 class inspection_default
  inspect <Protocol>

service-policy <Policy-map_name> interface <Interface_name> (Per Interface)
```

```
service-policy <Policy-map_name> global (Globally)
```
Àrevelia o ASA tem o **“global_policy”** permitido globalmente.

Configurar o Unicast Reverse Path Forwarding

```
ip verify reverse-path interface <interface_name>
```
Quando o tráfego obtém deixado cair devido à verificação RPF, da “a gota abaixo asp mostra” contrária no ASA incrementa.

```
ASA(config)# show asp drop

Frame drop:
 Invalid TCP Length (invalid-tcp-hdr-length)                  21
   Reverse-path verify failed (rpf-violated)                   90

// Check Reverse path statistics

ASA(config)# sh ip verify statistics
 interface inside: 11 unicast rpf drops
interface outside: 79 unicast rpf drops
```

Detecção da ameaça

A detecção da ameaça fornece administradores de firewall as ferramentas necessárias para identificar, compreender, e parar ataques antes que alcancem a infraestrutura de rede interna. A fim fazer assim, a característica confia em um número disparadores e de estatísticas diferentes, que é descrita em um detalhe mais adicional nestas seções.

Consulte por favor a funcionalidade e a configuração da detecção da ameaça ASA para a explicação de detalhe na detecção da ameaça no ASA.

Filtro de Botnet

Os pedidos e as respostas do Domain Name Server dos monitores do filtro de tráfego de BotNet (DNS) entre clientes dos DN internos e servidores DNS externos. Quando uma resposta de DNS é processada, o domínio associado com a resposta está verificado contra o base de dados de domínios maliciosos conhecidos. Se há um fósforo, todo o tráfego mais adicional ao endereço IP de Um ou Mais Servidores Cisco ICM NT atual na resposta de DNS está obstruído.

O malware é o software malicioso que é instalado em um host desavisado. O malware que tenta a atividade de rede tal como a emissão de dados privados (senhas, números do cartão de crédito, cursos chaves, ou dados proprietários) pode ser detectado pelo filtro de tráfego de Botnet quando o malware começa uma conexão a um endereço IP de Um ou Mais Servidores Cisco ICM NT ruim conhecido. O filtro de tráfego de Botnet verifica entrante e conexões de saída contra um base de dados dinâmico de Domain Name e de endereços IP de Um ou Mais Servidores Cisco ICM NT ruins conhecidos (a *lista negra*), e então logs ou obstrui toda a atividade suspeita.

Você pode igualmente suplementar o base de dados dinâmico de Cisco com os endereços põr da sua escolha adicionando os a uma lista negra estática; se o base de dados dinâmico incluir os endereços põr que você pensa se é põr, você pode manualmente incorporá-los em um *whitelist* estático. Os endereços de Whitelisted ainda gerenciem mensagens do syslog, mas porque você está visando somente mensagens do syslog da lista negra, são informativos. Consulte por favor configurando o filtro de tráfego de Botnet para a informação detalhada.

Adições do cache ARP para sub-redes NON-conectadas

Àrevelia o ASA não responde ao ARP para endereços IP de Um ou Mais Servidores Cisco ICM NT da sub-rede conectada NON-direto. Se você tem um IP NAT no ASA que não pertence ao IP da mesma sub-rede da relação ASA, nós teremos que permitir “a licença-nonconnected arp” no ASA ao Proxy-arp para o IP de NATted.

```
arp permit-nonconnected
```

Recomenda-se sempre ter o roteamento correto em dispositivos do fluxo acima e fluxo abaixo para que o NAT trabalhe sem permitir o comando acima.

Registro e monitoração

Configurando o SNMP

Esta seção destaca diversos métodos que podem ser usados a fim fixar o desenvolvimento do SNMP dentro dos dispositivos ASA. É crítico que o SNMP esteja fixado corretamente a fim proteger a confidencialidade, a integridade, e a Disponibilidade dos dados de rede e dos dispositivos de rede com que estes dados transitam por. O SNMP fornece-o uma riqueza de informação na saúde dos dispositivos de rede. Esta informação deve ser protegida dos usuários maliciosos que querem leverage estes dados a fim executar ataques contra a rede.

Strings de comunidade SNMP

Os string de comunidade são as senhas que são aplicadas a um dispositivo ASA para restringir o acesso, de leitura apenas e o acesso de leitura/gravação, aos dados SNMP no dispositivo. Estes strings de comunidade, como com todas as senhas, devem com cuidado ser escolhidos se assegurar de que não sejam triviais. Os strings de comunidade devem ser mudados em intervalos regulares e de acordo com políticas de segurança de rede. Por exemplo, as cordas devem ser mudadas quando um administrador de rede muda papéis ou deixa a empresa.

Permita o acesso de leitura SNMP:

```
snmp-server host <interface_name> <remote_ip_address>
```

Permita o SNMP traps

```
snmp-server enable traps all
```

Configurando o Syslog

Recomendou para enviar a informação de registro a um servidor de SYSLOG remoto. Isto torna possível correlacionar mais eficazmente e rede de auditoria e eventos de segurança através dos dispositivos de rede. Note que os mensagens do syslog estão transmitidos incerta pelo UDP e na minuta. Por este motivo, todas as proteções que uma rede tiver recursos para ao tráfego de gerenciamento (por exemplo, criptografia ou acesso out-of-band) devem ser prolongadas a fim incluir o tráfego do Syslog. Os logs podem ser cofnigured para ser ao seguinte destino do ASA:

- ASDM
- Buffer
- Flash

- Email
- Servidor FTP
- Servidor SNMP como armadilhas
- Server dos Syslog

Configurado o nível de seriedade do logging de console

```
logging console critical
```

O Syslog baseado TCP está igualmente disponível. Todos os Syslog podem ser enviados ao servidor de SYSLOG no texto simples ou dentro ser cifrados em caso do TCP.

Texto simples

syslog_ip do interface_name do logging host [porta tcp/

Cifrado

syslog_ip do interface_name do **logging host** [*porta* **tcp/** | [secure]

Se uma conexão de TCP não pode ser estabelecida com o server dos Syslog, todas as novas conexões estarão negadas. Você pode mudar este comportamento padrão incorporando “o comando da **licença-hostdown de registro”**.

Configurar Timestamps nos mensagens de registro

A configuração de data/hora de registro ajuda-o a correlacionar eventos através dos dispositivos de rede. É importante executar uma configuração correta e consistente de data/hora de registro assegurar-se de que você possa correlacionar dados de registo.

```
logging timestamp
```

Para relativo à informação adicional ao Syslog consulte por favor o exemplo de configuração do Syslog ASA.

Configurando o Netflow

Às vezes, você pode precisar de identificar rapidamente e tráfego de rede do retorno de monitoramento, especialmente durante a resposta do incidente ou o desempenho da rede deficiente. O NetFlow pode fornecer a visibilidade em todo o tráfego na rede. Adicionalmente, o NetFlow pode ser executado com coletores que podem fornecer a tensão do prazo e a análise automatizada.

Cisco ASA apoia serviços da versão 9 do Netflow. As aplicações ASA e ASASM de NSEL fornecem um stateful, o método de seguimento do fluxo IP que exporta somente aqueles registros que indicam eventos significativos em um fluxo. No fluxo do stateful que segue, os fluxos seguidos atravessam uma série de mudanças de estado. Os eventos NSEL são usados para exportar dados sobre o estado do fluxo e provocados pelo evento que causou a mudança de estado.

Consulte por favor o guia de execução do Netflow de Cisco ASA para mais informação do Netflow no ASA:

Fixando a configuração

Verificação da imagem no ASA

Partindo de 9.1(2) e de 8.4(4.1), o apoio para a verificação da integridade da imagem do SHA-512 foi adicionado. Para verificar a soma de verificação de um arquivo, use o comando verify no modo de exec privilegiado.

Calcula e indica o valor MD5 para a imagem do software especificada. Compare este valor com o valor disponível no cisco.com para esta imagem.

```
verify [ /md5 path ] [ md5-value ]
```

Senhas na configuração

Todas as senhas e as chaves são cifradas ou confundidas. Da “a executar-configuração mostra” não revela as senhas reais.

Tal backup não pode ser usado para o backup/restauração no ASA. O backup que é tomado para a restauração purposes o whould seja executado usando o comando “mais sistema: executar-configuração”. As senhas da configuração ASA podem ser cifradas usando uma frase de passagem mestra. Consulte por favor a criptografia de senha para a informação detalhada.

Preste serviços de manutenção à recuperação de senha

Desabilitar isto desabilitará o mecanismo da recuperação de senha e desabilitará o acesso ao ROMMON. Os únicos meios da recuperação de perdido ou das senhas esquecida serão para que o ROMMON apague todos os sistemas de arquivos que incluem arquivos de configuração e imagens. Você deve fazer um backup de sua configuração e ter um mecanismo para restaurar imagens da linha de comando rommon.

Troubleshooting

Não há nenhuma seção de Troubleshooting para este documento.