Melhore a Segurança no CSS11000 e no CSS11500

Índice

Introdução

Este documento fornece a informação sobre os ajustes da configuração Cisco que podem melhorar a Segurança no interruptor do Cisco Content Services (CSS) 11000 ou CSS11500. Este documento descreve os ajustes da configuração básica que são quase universalmente aplicáveis nas redes IP e cobre alguns artigos inesperados de que você deve estar ciente.

Este documento não apresenta uma lista exaustiva destes artigos, nem pode a informação no documento ser substituída para o conhecimento da parte do administrador de rede. O documento serve como um lembrete dos artigos que são esquecidos às vezes.

Este documento menciona somente os comandos que são importantes nas redes IP. Muitos dos serviços que você pode permitir no CSS exigem a configuração de segurança cuidadosa. Contudo, este documento centra-se sobre a informação para os serviços que são permitidos à revelia ou que são permitidos quase sempre por usuários e que pode exigir a incapacidade ou a reconfiguração.

Algumas das configurações padrão no software webns de Cisco existem para razões históricas. Estes ajustes eram aplicáveis quando foram escolhidos, mas eram provavelmente diferentes se os padrões novos foram escolhidos hoje. Outros padrões são aplicáveis para a maioria de sistemas, mas podem criar exposições de segurança se estes padrões são usados nos dispositivos que formam parte de uma defesa de perímetro de rede. Outros padrões são exigidos ainda realmente por padrões, mas não são sempre desejáveis de um ponto de vista de segurança.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

Convenções

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

Gerenciamento de senha

As senhas e a informação proprietária similar, tal como string de comunidade do Simple Network Management Protocol (SNMP), são a defesa principal contra o acesso não autorizado a seu CSS. A melhor maneira de tratar a maioria das senhas é mantê-las em um servidor de autenticação TACACS+ ou RADIUS. Contudo, quase cada CSS ainda tem uma senha localmente configurada para o acesso de privilegiado. O CSS pode igualmente incluir a outra informação de senha no arquivo de configuração. Toda a senha que for configurada no texto claro aparece na configuração cifrada com Data Encryption Standard (DES).

Perfis de usuário local

Esta lista descreve os perfis de usuário local:

- *Administrador* — O perfil do administrador inclui estes privilégios:Acesso ao menu de monitor de diagnóstico off-lineAcesso direto à linha de comandoAcesso de diretório completoEstes ajustes podem ser configurados da linha de comando ou do menu de monitor de diagnóstico off-line.
- *Técnico* — O perfil do técnico inclui estes privilégios:Acesso direto à linha de comandoAcesso de diretório completoEstes ajustes podem ser configurados com uso da linha de comando. Não use o perfil do técnico para propósitos administrativos CSS.
- *Superuser* — O perfil do Superuser inclui estes privilégios:Acesso direto à linha de comandoA capacidade para salvar limitações do acesso de diretórioEstes ajustes podem ser configurados com uso da linha de comando.
- *Usuário* — O perfil de usuário não pode fazer alterações de configuração e inclui limitações do acesso de diretório. Estes ajustes podem ser configurados com uso da linha de comando.

Quando você emite o **comando restrict user-database**, você reforça limitações do acesso de diretório em cada usuário. Os níveis de usuário somente do administrador e do técnico podem executar estas ações:

- Remova o **comando restrict user-database**.
- Mude o **comando local user-database**.
- Emita o **comando clear running-config**.

Controle do acesso interativo

Todo o usuário que puder entrar a um CSS pode o Exibir informação que o público em geral não precisa necessariamente de ver. Em alguns casos, um usuário que possa entrar ao CSS pode usar o CSS como um relé para futuros ataques de rede. Um usuário que ganhe o acesso de privilegiado ao CSS pode reconfigurar o CSS. A fim impedir o acesso impróprio, você precisa de controlar login interativo ao CSS.

Embora a maioria de acesso interativo seja desabilitado à revelia, há umas exceções. As exceções as mais óbvias são sessões interativa diretamente dos terminais assíncronos conectados, tais como o terminal de console, e acesso à porta de gerenciamento de Ethernet.

Refira configurar métodos do Acesso remoto CSS para obter mais informações sobre de como controlar o acesso interativo ao CSS.

Portas do console

Um artigo importante a recordar é que a porta de Console de um dispositivo Cisco tem privilégios especiais. Em particular, supõe que alguém envia um caráter ESC (escape) à porta de Console quando a corrida dos diagnósticos do CARGO. Depois que uma repartição, esta pessoa pode facilmente usar o procedimento de recuperação de senha a fim tomar o controle do sistema. Os atacantes que podem interromper a potência ou induzem um travamento de sistema, e que têm o acesso à porta de Console através de um terminal embutido através de componente de hardware, de um modem, de um servidor terminal, ou de algum outro dispositivo de rede, podem tomar o controle do sistema. Estes atacantes podem tomar o controle mesmo se não têm o acesso físico ao sistema ou à capacidade entrar normalmente ao sistema.

Consequentemente, todo o modem ou dispositivo de rede que derem o acesso à porta de Console da Cisco devem ser fixados a um padrão que seja comparável à Segurança que é usada para o acesso de privilegiado ao CSS. Pelo menos, todo o modem do console deve ser de um tipo que possa exigir o usuário dialup fornecer uma senha para o acesso, e a senha de modem deve com cuidado ser controlada.

Acesso interativo geral

Há mais maneiras de obter conexões interativa a um CSS do que usuários pode realizar. Você pode usar estes métodos a fim controlar o CSS:

- Telnet
- Host do Secure Shell (SSH)
- SNMP:
- Console
- FTP
- XML
- Gerenciamento de web

Emita o **comando restrict** a fim permitir ou desabilitar. O CSS ainda escuta na porta particular, mas fecha a conexão. De modo que os pacotes não batam estas portas, configurar cláusulas do Access Control List (ACL) para negar os pacotes.

Édifícil estar absolutamente certo que todos os modos possíveis de acesso estiveram obstruídos. Na maioria dos casos, os administradores devem usar algum meio mecanismo da autenticação a fim certificar-se de que os inícios de uma sessão em todas as linhas são controlados. Os administradores devem assegurar-se de que os inícios de uma sessão estejam controlados mesmo nas máquinas que são supostas para ser inacessíveis das redes não confiável.

Controle do acesso de console

Àrevelia, o console autentica contra perfis de usuário localmente configurados. A fim ativar o TACACS+ ou a autenticação RADIUS, emita o comando global da **autenticação do console** e as opções associadas.

Controle dos VTY

Àrevelia, os vtys autenticam contra perfis de usuário localmente configurados. A fim ativar o TACACS+ ou a autenticação RADIUS, emita o comando global da **autenticação virtual** e as opções associadas.

Apoio SSH

Se seus suportes de software um protocolo do acesso criptografado tal como o SSH, Cisco recomendam que você permite somente esse protocolo e desabilite o acesso do telnet quando você quer usar o servidor de SSH. A fim permitir o demônio SSH (SSHD), você precisa uma licença de servidor SSHD, que permita a funcionalidade SSHD no padrão e em versões aprimorada do software CSS. Emita os **comandos sshd**. Refira configurar protocolos de rede CSS para mais informação.

Nota: Apoio da versão de SSH 1 começado em 4.01. Apoio da versão de SSH 2 começado em 5.20.

RADIUS

Até à data da versão 5.00 e mais recente, você pode configurar o CSS para usar o RAIO para a autenticação de usuário. A fim configurar o CSS para a autenticação RADIUS, refira configurar perfis de usuário e Parâmetros CSS.

Nota: Um usuário/perfil de grupo exige somente atributos RADIUS do Internet Engineering Task Force (IETF), tipo de serviço [006] = administrativo.

Esta lista identifica os códigos da mensagem debugar:

```
PW_ACCESS_REQUEST       1
PW_ACCESS_ACCEPT        2
PW_ACCESS_REJECT        3
PW_ACCOUNTING_REQUEST   4
PW_ACCOUNTING_RESPONSE  5
PW_ACCOUNTING_STATUS    6
PW_ACCESS_CHALLENGE     11
```

A fim ver debuga que são associados com os login radius, emitem estes comandos:

```
logging subsystem radius level debug-7
logging subsystem security level debug-7
logging subsystem netman level debug-7
```

Este é um exemplo de uma autenticação bem sucedida debuga:

```
logging subsystem radius level debug-7
logging subsystem security level debug-7
logging subsystem netman level debug-7
```

Este é um exemplo de uma autenticação que falhe devido a um nome de usuário incorreto ou a uma senha:

```
logging subsystem radius level debug-7
logging subsystem security level debug-7
logging subsystem netman level debug-7
```

Este é um exemplo de uma autenticação que falhe porque o tipo de serviço do atributo RADIUS 006 do perfil de usuário não é configurado:

```
logging subsystem radius level debug-7
logging subsystem security level debug-7
```

```
logging subsystem netman level debug-7
```

TACACS+

Na versão 5.03 e mais recente, você pode configurar o CSS para usar o TACACS+ para a autenticação de usuário. A fim configurar o CSS para a autenticação TACACS+, refira os Release Note para o Cisco CSS 11000 series.

A fim ver debuga que são associados com os inícios de uma sessão TACACS+, emitem estes comandos:

```
logging subsystem security level debug-7
logging subsystem netman level debug-7
```

Este é um exemplo de uma autenticação bem sucedida debuga:

```
logging subsystem security level debug-7
logging subsystem netman level debug-7
```

Este é um exemplo de uma autenticação falha devido a um nome de usuário incorreto ou a uma senha:

```
logging subsystem security level debug-7
logging subsystem netman level debug-7
```

Banners de advertência

Em algumas jurisdições, você pode extremamente facilitar o processo de civil e/ou o processo criminal de biscoitos que quebram em seus sistemas se você fornece uma bandeira que informe usuários não autorizados que seu uso é desautorizado. Outras jurisdições proibem o monitor das atividades mesmo de usuários não autorizados a menos que você tomar etapas para notificar usuários de sua intenção para fazer assim. Uma maneira de fornecer esta notificação é pô-la em um mensagem de banner. Você pode configurar um mensagem de banner com o **comando set banner** CSS. Este comando foi introduzido em 5.03.

Os requisitos de notificação legais são complexos e variam em cada jurisdição e situação. Mesmo dentro das jurisdições, as opiniões legais variam. Discuta esta edição com seu advogado. Em colaboração com o conselho, considere qual destas observações pôr em sua bandeira:

- Uma observação que especificamente os pessoais autorizados dos estados somente devem entrar a ou usar o sistema e talvez a informação sobre quem pode autorizar o uso.
- Uma observação que toda a utilização não autorizada do sistema é ilegal e pode ser sujeita a civil e/ou às penalidades criminal.
- Uma observação que algum uso do sistema pode ser registrado ou monitorado sem aviso futuro e que os log resultante podem ser usados como a evidência no tribunal.
- Observações específicas que são exigidas por leis local.

Para razões da Segurança (um pouco do que legal), não inclua em seu banner de login esta informação sobre seu CSS:

- Nome
- Modelo
- Software que é executado
- Proprietário

Serviços de gerenciamento comumente configurados

Muitos usuários controlam suas redes com o uso dos protocolos diferentes do login interativo remoto. Os protocolos mais comuns para esse fim são SNMP e HTTP. A maioria de opção segura não é permitir estes protocolos de todo. Contudo, se você permitiu um dos protocolos, fixe-o como esta seção descreve.

SNMP:

O SNMP é muito amplamente utilizado para o dispositivo de rede que monitora e, frequentemente, para alterações de configuração. O SNMP tem duas revisões padrão principais, SNMPv1 e SNMPv2. Seu CSS suporta versão SNMP 2C (SNMPv2C), que é sabido como o SNMP comunidade-baseado. O CSS gerencie armadilhas no formato SNMPv1.

A fim controlar o acesso SNMP ao CSS, emita o **comando no restrict snmp** e o **comando restrict snmp**. O acesso com o SNMP é permitido à revelia. Se você desabilita o acesso com o SNMP, o CSS ainda escuta na porta particular 1, mas fecha a conexão. Configurar cláusulas ACL para negar os pacotes de modo que os pacotes não batam a porta SNMP.

Infelizmente, o SNMPv1 e o SNMPv2C usam um esquema de autenticação muito fraca que seja baseado em um string de comunidade. A autenticação atinge uma senha fixa que seja transmitida sobre a rede sem criptografia. Se você deve usar o SNMPv2C, seja cuidadoso escolher string de comunidade obscuros (e não use, por exemplo, público ou privado). Se em todo o possível, evite o uso dos mesmos string de comunidade para todos os dispositivos de rede. Use uma corda ou umas cordas diferentes para cada dispositivo, ou pelo menos para a cada área da rede. Não torne uma seqüência de somente leitura igual a uma de leitura e gravação. Se possível, faça a votação periódica SNMPv2C com uma série de comunidade de somente leitura. As séries de leitura/gravação do uso somente para real escrevem operações.

O SNMPv2C não é apropriado de usar-se por estas razões através dos Internet públicas:

- O SNMPv2C usa séries de autenticação de cleartext.
- O SNMPv2C é um protocolo de transação baseado em conjunto de dados que seja facilmente falsificado.
- A maioria das implementações SNMP envia essas séries repetidamente como parte de uma eleição periódica.

Considere com cuidado as implicações antes que você use o SNMPv2C através dos Internet públicas.

Na maioria de redes, os mensagens snmp legítimo vêm somente das determinadas estações de gerenciamento. Se os mensagens snmp legítimo vêm somente das determinadas estações de gerenciamento em sua rede, considere o uso dos ACL que são aplicados aos VLAN de circuito a fim negar mensagens SNMP indesejado.

As estações de gerenciamento de SNMP costumam possuir grandes bancos de dados de informações de autenticação, como séries de comunidade. Esta informação pode fornecer o acesso a muitos CSS e a outros dispositivos de rede. Esta concentração de informação faz o gerenciamento de SNMP postar um destino natural para o ataque. Fixe a estação do gerenciamento de SNMP em conformidade.

HTTP

O CSS apoia a configuração remota através do protocolo HTTP com uso de documentos do linguagem de marcação extensível (XML). Na versão webns 4.10 ou mais adiantado, você pode alcançar o acesso às interfaces do utilizador do Gerenciamento de dispositivos de WebNS no texto claro se você consulta à porta TCP 8081. Geralmente, o acesso HTTP é equivalente ao acesso interativo ao CSS. O protocolo de autenticação que é usado para o HTTP é equivalente à emissão de uma senha de texto claro através da rede. Infelizmente, não há nenhuma disposição eficaz no HTTP para desafio-baseado ou senhas de uma vez. Consequentemente, o HTTP é relativamente uma opção de risco para o uso através dos Internet públicas.

Se você escolhe usar o HTTP para o Gerenciamento, restrinja o acesso aos endereços IP de Um ou Mais Servidores Cisco ICM NT apropriados com o uso dos ACL que são aplicados aos VLAN de circuito. A fim controlar o acesso HTTP XML ao CSS, emita o **comando no restrict xml** e o **comando restrict xml**. Em umas versões mais atrasadas de WebNS, o comando mudou ao **estado Web-MGT** *[desabilitação | permita]*. O acesso com HTTP XML é desabilitado à revelia. A fim controlar o acesso de usuário do Gerenciamento de dispositivos HTTP WebNS, emita o **comando no restrict web-mgmt** e o **comando restrict web-mgmt**. A interface do utilizador do Gerenciamento de dispositivos de WebNS é desabilitada à revelia. Você deve configurar o **comando no restrict xml** e o **comando no restrict web-mgmt** a fim consultar ao CSS na porta 8081.

Na versão 5.00 e mais recente, se você HTTP-consulta ao endereço do circuito na porta 8081, o navegador é reorientado para usar o HTTPS e conectá-lo ao mesmo endereço do circuito.

HTTPS

O CSS apoia a configuração remota com o protocolo seguro HTTP (HTTPS). Este Secure Socket Layer (SSL) protege transferências de dados (que podem incluir senhas) entre a interface do utilizador do Gerenciamento de dispositivos de WebNS e seu navegador da Web.

A fim controlar o acesso de usuário do Gerenciamento de dispositivos HTTPS WebNS, emita o **comando no restrict web-mgmt** e o **comando restrict web-mgmt**. A interface do utilizador do Gerenciamento de dispositivos de WebNS é desabilitada à revelia. Se é desabilitada, o CSS continua a escutar na porta particular mas fecha a conexão. De modo que os pacotes não batam a porta TCP 443 SSL, configurar cláusulas ACL para negar os pacotes.

Gerenciamento e acesso interativo sobre o Internet (e outras redes não-confiável)

Muitos usuários controlam seus CSS remotamente, e às vezes este é realizado sobre o Internet. Qualquer tipo de acesso remoto não criptografado oferece riscos, mas o acesso em uma rede pública, como a Internet, é especialmente perigoso. Todos os esquemas de gerenciamento remotos, que incluem o acesso interativo, o HTTP, e o SNMP, são vulneráveis.

Os ataques que esta seção discute são os relativamente sofisticados, mas eles são de modo algum fora do alcance dos biscoitos de hoje. Os provedores de rede públicas que tomam as medições de segurança adequadas podem frequentemente estragar estes atacantes. Avalie seu nível de confiança nas medidas de segurança que todos os fornecedores que levam seu uso do tráfego de gerenciamento. Mesmo se você confia seus fornecedores, tomada pelo menos algumas etapas para proteger-se dos resultados de alguns erros que estes fornecedores pudessem fazer.

Todos os cuidados nesta seção aplicam tanto quanto aos anfitriões a respeito do CSS. Quando

este documento discutir como proteger as sessões de login CSS, igualmente olham no uso dos mecanismos analógicos a fim proteger seus anfitriões se você administra aqueles anfitriões remotamente. A administração de Internet remota é útil, mas exige a atenção cuidadosa à Segurança.

Farejadores de pacote

Os biscoitos quebram frequentemente nos computadores que os provedores de serviço da Internet possuem, ou em computadores em outras redes grandes. Os biscoitos instalam os programas do rastreamento de pacote, que monitoram o tráfego que passa através da rede. Estes programas do rastreamento de pacote roubam dados, tais como senhas e séries de comunidade snmp. Os operadores de rede começaram a melhorar sua Segurança, que faz este roubo mais difícil. Contudo, este roubo é ainda relativamente comum. Além do que o risco dos invasores exteriores, os pessoais de ISP de rogue podem igualmente instalar tubos aspiradores. Toda a senha que for enviada sobre um canal não criptografado é em risco, que inclua o início de uma sessão e permite senhas para seus CSS.

Se você pode, para evitar registrar em seu CSS com o uso de algum protocolo não criptografado sobre alguma rede não confiável. Se seu software CSS a apoia, use um protocolo de login criptografado tal como o SSH.

Se você não tem o acesso a um protocolo de acesso remoto cifrado, uma outra possibilidade é usar um sistema de senha de uma vez tal como o S/KEY ou o OPIE, junto com um TACACS+ ou um servidor Radius, a fim controlar login interativo e acesso de privilegiado a seu CSS. A vantagem é que uma senha roubada é inútil. Uma senha roubada é feita inválida pela mesma sessão em que é roubada. Os dados que são transmitidos na sessão e não relativo às senhas permaneça disponível aos eavesdropperes, mas muitos programas do sniffer estabelecem-se para concentrar-se em senhas.

Se você deve enviar sessões de Telnet das senhas em texto sem formatação, mude suas senhas frequentemente. e toda atenção do pagamento ao trajeto que suas sessões atravessam.

Outros perigos de acesso à Internet

Além do que rastreamentos de pacote, o gerenciamento de Internet remoto de um CSS apresenta estes riscos de segurança:

- A fim controlar um CSS sobre o Internet, você deve permitir pelo menos alguns host de Internet ter o acesso ao CSS. Estes anfitriões podem ser comprometidos, ou seus endereços podem ser falsificado. Quando você permite o acesso interativo do Internet, você faz sua segurança dependente, não somente em suas próprias medidas da antifalsificação, mas nas medidas da antifalsificação dos provedores de serviços que são involvidos.Você pode reduzir estes perigos se você executa estas ações:Certifique-se de que todos os anfitriões que são permitidos para entrar a seu CSS estão sob seu próprio controle.Use protocolos de login criptografado com autenticação forte.
- Às vezes, o acesso a uma conexão TCP não criptografada (tal como uma sessão de Telnet) é possível para obter. Alguém que obtém o acesso a este tipo de sessão pode realmente tomar o controle longe de um usuário que seja entrado. Tais ataques não são quase tão comuns quanto o sniffing do pacote simples e podem ser complexos montar. Contudo, tais ataques são possíveis, e um atacante que tenha sua rede especificamente na mente

enquanto um alvo pode os usar. A única solução real ao problema de roubo de sessão é usar um protocolo de gestão fortemente autenticado, cifrado.
- O ataque de recusa de serviço (DOS) é relativamente comum no Internet. Se sua rede está sob um ataque DoS, você pode ser incapaz de alcançar seu CSS a fim recolher a informação ou tomar a ação defensiva. Mesmo um ataque na rede de alguma outra pessoa pode danificar o acesso de gerenciamento a sua própria rede. Embora você possa tomar etapas para fazer sua rede mais resistente aos ataques DoS, a única defesa real contra este risco é ter um separado, canal de gerenciamento out-of-band (tal como um modem dialup) para o uso nas emergências.

Registro

Cisco CSS enlata a informação de registro sobre uma variedade de eventos, muitos de que tenha o significado de segurança. Os logs podem ser inestimáveis para a caracterização e a resposta aos incidentes de segurança. Você pode emitir o **comando logging subsystem** a fim permitir entra o CSS. O nível de registro do padrão é warning-4 para todos os subsistemas.

Emita estes comandos para que a ordem de abertura do subsistema recolha esta informação:

- Login de usuário
- Saídas
- Autenticação RADIUS
- Autenticação TACACS+

```
logging subsystem radius level debug-7
logging subsystem security level debug-7
logging subsystem netman level debug-7
```

Nota: As tampas TACACS+ do **comando netman subsystem** debugam.

De um ponto de vista de segurança, os eventos os mais importantes que os registros do logging do sistema geralmente incluem estes eventos:

- Mudanças do status da interface
- Mudanças à configuração de sistema
- Fósforos ACL

```
logging subsystem netman level info-6
!--- Note that the default logging level is warning-4, which does !--- not appear in the
configuration. logging commands enable
logging subsystem acl level debug-7
```

O Remote Monitoring (RMON) permite-o remotamente monitora e analisa a atividade de pacotes em portas Ethernet CSS. O RMON igualmente permite a configuração do alarme para o monitor dos objetos MIB e permite que a configuração de evento notifique-o destas condições de alarme. Um evento de RMON é a ação que ocorre quando um alarme de RMON associado é provocado. Você pode configurar um evento do alarme tais que, quando um evento do alarme ocorre, gerencie um ou both of these artigo:

- Um evento do log
- Uma armadilha a uma estação de gerenciamento de rede SNMP

Salvar a informação de registro

Àrevelia, o CSS salvar mensagens de Log de evento da bota e do subsistema aos arquivos de registro no duro ou no disco flash. O índice destes arquivos é gravado no texto de ASCII. Você pode igualmente configurar o CSS para enviar mensagens de registro a uma sessão ativa de CSS, ao endereço email, ou a um outro sistema host.

O tamanho máximo de um arquivo de Log é 50 MB para sistemas disco-baseados duros e 10 MB para sistemas disco-baseados flash.

Os mensagens de registro do subsistema são os eventos do subsistema que ocorrem durante a operação do CSS. O CSS salvar estas mensagens no arquivo de sys.log. O CSS cria este arquivo quando o primeiro evento do subsistema ocorre que deve ser registrado. O CSS determina que mensagens de subsistema a registrar por seu nível de registro configurado.

A maioria de instalações maiores têm servidores de SYSLOG. Você pode emitir o **comando logging host** a fim enviar a informação de registro a um demônio do Syslog no sistema host. Mesmo se você tem um servidor de SYSLOG, você deve ainda permitir o logging local ao disco.

Todos os logs tempo-são carimbados com o mês, dia, e cronometram ao segundo. Se você configura uma fonte do tempo comum tal como o protocolo de tempo de rede simples (SNTP) para seus logs, você pode mais facilmente seguir a sequência de eventos registrados. A fim configurar o servidor SNTP no CSS, emita o **comando sntp**. O SNTP foi introduzido no código 5.00.

Grave violações da lista de acesso

Se você usa ACL ao filtrar tráfego que alcança endereços do circuito ou endereços do IP virtual da regra de conteúdo (VIP), você pode escolher registrar os pacotes que violam seus critérios do filtro. A fim permitir a abertura da cláusula ACL, emita o **comando clause - log enable**. Também, emita o **comando logging subsystem acl level debug-7**. O CSS registra esta informação:

- Protocolo
- Porta de origem
- Porta do destino
- Endereço IP de origem
- Endereço IP de destino

Tente evitar a configuração do registro para as entradas ACL que combinam muito um grande número pacotes. Esta configuração faz com que os arquivos de registro cresçam excessivamente grandes e pode cortar no desempenho de sistema.

Você pode igualmente usar o logging ACL para caracterizar o tráfego que é associado com os ataques de rede. Neste caso, você configura o logging ACL para registrar o tráfego suspeito. Você pode caracterizar no roteador Cisco no lado do Internet do CSS a fim craft um ACL. Refira a caracterização e inundações de pacote de informação de seguimento usando roteadores Cisco para mais informação.

Nota: O CSS ACL é aplicado somente em pacotes de entrada. O ACL não verifica os pacotes que são de partida de uma relação.

Fixe Roteamento IP

Esta seção discute algumas medidas de segurança básica que se relacionam à maneira em que do roteador os pacotes IP para a frente. Refira ISP Cisco essenciais - Os IO essenciais caracterizam cada ISP devem considerar para obter mais informações sobre destas edições.

Àrevelia, uma configuração do CSS:

- Restringe o número de pacotes SYN que vão a um VIP antes que o CSS o registre como um ataque DoS**Nota:** Este comportamento não pode ser desabilitado.
- Nega transmissões direcionada
- Nega pacotes com o mesmo endereço IP de origem e de destino
- Nega endereços IP de Um ou Mais Servidores Cisco ICM NT do origem de transmissão múltipla
- Nega a porta de origem ou destino 0 pacotes

Antifalsificação

Muitos ataques de rede confiam em um atacante que falsifique, ou em paródias, os endereços de origem de datagramas IP. Alguns ataques confiam na falsificação para que o ataque trabalhe. Os outros ataques são muito mais duros de seguir se os atacantes podem usar o endereço de alguma outra pessoa em vez de seu próprio endereço. Consequentemente, impedir a falsificação onde quer que é praticável é valioso para administradores de rede.

A antifalsificação deve ser feita em cada ponto na rede onde é prática. Mas a antifalsificação é geralmente a mais fácil de fazer e o mais eficaz nas beiras entre grandes blocos de endereço ou entre domínios da administração de rede. A antifalsificação em cada roteador em uma rede é geralmente pouco prática porque a determinação de que os endereços de origem podem legitimamente aparecer em toda a dada interface é difícil.

Se você é um provedor de serviço do Internet (ISP), você pode encontrar que anti-falsificação efetiva, junto com outras medidas de segurança eficazes, as causas caras, assinantes com problema tomar seu negócio a outros fornecedores. Se você é um ISP, seja especialmente cuidadoso aplicar controles da antifalsificação em associações do tratamento por imagens e em outros pontos de conexão do utilizador final.

Nota: Refira o RFC 2267 .

Os administradores dos firewall corporativa ou dos roteadores de perímetro instalam às vezes medidas da antifalsificação de modo que os anfitriões no Internet não possam supor os endereços de host interno. Contudo, os host internos podem ainda supor os endereços dos anfitriões no Internet. Tente impedir a falsificação nos ambos sentidos. Há pelo menos três bons motivos instalar a antifalsificação nos ambos sentidos em um firewall organizacional:

- Os usuários internos estão tentados menos tentar lançar ataques de rede e menos provável suceder se tentam.
- Os host internos que são desconfigurados acidentalmente são menos prováveis causar o problema para locais remotos. Consequentemente, são menos prováveis gerar o insatisfação do cliente.
- Invasores externos geralmente se dividem em redes como preenchimentos de inicialização para outros ataques. Esses invasores podem estar menos interessados em uma rede com proteção contra falsificação de saída.

Antifalsificação com ACL

Infelizmente, simplesmente aos comandos list que fornecem a proteção anti-falsificação apropriada não é prática. A configuração ACL depende demasiado da rede individual. O objetivo básico é rejeitar os pacotes que chegam nas relações que não são trajetos viáveis dos endereços de origem supostos daqueles pacotes. Por exemplo, em um dois-circuito CSS que conecte uma fazenda do server ao Internet, você quer rejeitar toda a datagrama que chegar no circuito do Internet, mas tem um campo de endereço de origem que reivindique que veio de uma máquina na fazenda do server.

Similarmente, você quer rejeitar toda a datagrama que chegar na relação que são conectadas à fazenda do server, mas que tem um campo de endereço de origem que reivindique que veio de uma máquina fora da fazenda do server. Se os recursos do CPU reservam, aplique a antifalsificação em todo o circuito onde uma determinação do que tráfego possa legitimamente chegar é praticável.

Os ISP que levam o tráfego de trânsito podem ter limitado oportunidades de configurar a antifalsificação ACL, mas tais ISP podem geralmente filtrar fora do tráfego que reivindica originar dentro do espaço de endereços desse ISP.

Geralmente, os filtros da antifalsificação devem ser construídos com entradas ACL. Os pacotes devem ser filtrados nos circuitos através de que os pacotes chegam. O CSS pode somente aplicar ACL aos pacotes de entrada.

Quando a antifalsificação ACL existe, devem sempre rejeitar datagramas com transmissão ou endereços de origem de transmissão múltipla. À revelia, o CSS nega estas datagramas. A antifalsificação ACL deve igualmente rejeitar as datagramas que têm o endereço de loopback reservado como um endereço de origem. Além, você deve geralmente mandar uma antifalsificação ACL filtrar para fora todo o Internet Control Message Protocol (ICMP) reorienta, apesar do endereço de origem ou de destino. O CSS ACL não permite que você especifique o tipo ICMP para negar. Em lugar de, emita o **comando no redirects** a fim configurar todos os endereços IP de circuito para não aceitar redirecionamentos de ICMP. Estes são os comandos:

```
clause # deny any 127.0.0.0 255.0.0.0 destination any
clause # deny any 0.0.0.0 0.0.0.0 destination any
```

Nota: A cláusula # nega todo o comando any do destino de 0.0.0.0 0.0.0.0 filtra para fora pacotes de muitos clientes do protocolo de bootstrap (BOOTP) /DHCP. Consequentemente, o comando não é apropriado em todos os ambientes.

Controle das transmissões direcionada

Ataques extremamente comum e populares DoS do smurf, e alguns ataques relacionados, broadcasts direto de IP do uso. À revelia, o CSS é configurado com o **comando no ip subnet-broadcast**, que nega transmissões direcionada.

Um broadcast direto de IP é uma datagrama que seja enviada ao endereço de broadcast de uma sub-rede a que a máquina de envio não é anexada diretamente. A transmissão direcionada está distribuída através da rede como um pacote do unicast até que a transmissão direcionada chegue na sub-rede de destino. Na sub-rede, a transmissão direcionada é convertida em uma transmissão da camada de enlace. Devido à natureza da arquitetura do endereçamento de IP, somente o último roteador ou mergulha 3 que o dispositivo de rede na corrente pode

conclusivamente identificar uma transmissão direcionada. Este dispositivo é esse que é conectado diretamente à sub-rede de destino. As transmissões direcionadas são utilizadas ocasionalmente para finalidades legitimas, mas tal uso não é comum fora do setor de serviços financeiros.

Em um ataque de smurf, o atacante envia requisições de eco ICMP de um endereço de origem falsificado a um endereço de broadcast direcionado. Em consequência, todos os anfitriões na sub-rede de destino enviam respostas ao origem falsificada. Quando um atacante envia um fluxo contínuo de tal requisição, o atacante pode criar um fluxo de resposta muito maior, que possa completamente inundar o host cujo o endereço é falsificado.

Refira o mais atrasado no ataque de recusa de serviço: Descrição e informação de “Smurf” para minimizar efeitos para que uma estratégia obstrua ataques de smurf em alguns roteadores de firewall (que depende do projeto de rede). O documento igualmente fornece a informação geral no ataque de smurf.

Integridade do caminho

Muitos ataques dependem da capacidade para influenciar os trajetos que as datagramas tomam através da rede. Se os biscoitos controlam o roteamento, há uma possibilidade que podem spoof o endereço da máquina de um outro usuário e para ter o tráfego de retorno enviado a eles. Em alguns casos, os biscoitos podem interceptar e ler os dados que são pretendidos para alguma outra pessoa. O roteamento pode igualmente ser interrompido puramente para finalidades DoS.

Roteamento do origem de IP

O protocolo IP apoia as opções de roteamento de origem que permitem que o remetente de um IP datagram controle a rota que a datagrama toma para o destino final, e geralmente, a rota que toda a resposta toma. Essas opções são raramente utilizadas para fins legítimos em redes reais. Algumas implementações IP mais velhas não processam pacotes roteado de origem corretamente. Alguém pode enviar datagramas com opções de roteamento de origem e, para causar um crash possivelmente as máquinas que executam estas aplicações.

O CSS é configurado à revelia com o **comando no ip source-route set**. O CSS nunca para a frente um pacote IP que leve uma opção de roteamento de origem. Deixe o comando default configurado a menos que você souber que sua rede precisa o roteamento de origem.

Redirecionamentos de ICMP

Uma mensagem do redirecionamento de ICMP instrui um nó final para usar um roteador específico como o trajeto a um destino particular. Em uma rede IP que funcione corretamente, um roteador envia reorienta somente aos anfitriões nas sub-redes local do roteador. O nó final nunca envia uma reorientação, e reorienta-a nunca atravessa mais de um salto de rede. Contudo, um atacante pode violar estas regras, e alguns ataques são baseados nestas regras. Filtre para fora redirecionamentos de ICMP entrantes nas interfaces de entrada de todo o roteador que se encontrar em uma beira entre campos administrativos. Além, você pode ter todo o ACL que for aplicado no lado de entrada de uma interface de roteador Cisco filtra para fora todos os redirecionamentos de ICMP. Isto que filtra não causa nenhum impacto operacional em uma rede que seja configurada corretamente.

Este tipo de filtração impede reorienta somente os ataques que os atacantes remotos lançam.

Além, os atacantes podem usar-se reorientam para causar o problema significativo se o host do atacante é conectado diretamente ao mesmo segmento que um host que esteja sob o ataque.

Àrevelia, o CSS é configurado para aceitar reorienta em cada endereço IP de circuito que é configurado. Emita o **comando no redirect** sob o endereço IP de circuito a fim desligar esta função.

Filtro e Autenticação do Routing Protocol

Se você usa um protocolo de roteamento dinâmico que apoie a autenticação, permita essa autenticação. A autenticação impede alguns ataques maliciosos na infraestrutura de roteamento e pode igualmente ajudar a impedir dano que os dispositivos de rogue desconfigurados na rede podem causar.

Para as mesmas razões, os provedores de serviços e outros operadores das redes grandes podem considerar o uso do filtragem de rota. Com filtragem de rota, os roteadores de rede não aceitam claramente a informação de roteamento incorreta. Para o filtragem de rota, use o parâmetro da distribuir-**lista no** comando. O USO excessivo da filtragem de rota pode destruir as vantagens do roteamento dinâmico. Mas o uso seletivo ajuda frequentemente a impedir resultados ruins. Por exemplo, se você usa um protocolo de roteamento dinâmico a fim se comunicar com uma rede cliente do stub, não aceite nenhuma rotas desse cliente a não ser rotas ao espaço de endereços que você delegou realmente ao cliente.

O CSS não pode rotas de filtro. Em lugar de, configurar routing peer do CSS com esta função.

Este documento não fornece a instrução detalhada na configuração da autentificação de roteamento e do filtragem de rota. Tal documentação está disponível no cisco.com e em outra parte. Você pode referir os ISP Cisco essenciais do documento - os IO essenciais caracterizam cada ISP devem considerar. Devido à complexidade, procure conselho experiente se você é um principiante antes que você configure estas características em redes importantes.

Gerenciamento de inundação

Muitos ataques DoS confiam em inundações de pacote inútil. Estas inundações congestionam os enlaces da rede, tornam os hosts lentos e podem sobrecarregar os roteadores também. A configuração cuidadosa do roteador pode reduzir o impacto de tais inundações.

Uma parte importante do gerenciamento de inundação é a conscientização de onde os gargalos de desempenho podem ocorrer. Se uma inundação sobrecarrega uma linha T1, filtre para fora a inundação no roteador na extremidade de origem da linha. Há quase nenhum efeito se você filtra na extremidade de destino neste caso. Se o roteador próprio é a maioria de componente de rede sobrecarregada, você pode fazer matérias mais ruins se você filtra as proteções que colocam demandas pesadas no roteador. Mantenha isto na mente quando você considera uma aplicação das sugestões nesta seção.

Inundações de trânsito

Você pode usar características de QoS de Cisco no Roteadores ascendente do ® do Cisco IOS a fim proteger o CSS, os anfitriões, e os links contra alguns tipos das inundações. Infelizmente, este documento não fornece um tratamento geral deste meio gerenciamento de inundação. Também, a proteção depende pesadamente do ataque. O único simples, geralmente o conselho aplicável é

usar o Weighted Fair Queuing (WFQ) onde quer que os recursos do CPU podem apoiar o WFQ. O WFQ é o padrão para linhas do serial de baixa velocidade em umas versões de Cisco IOS Software mais atrasadas. Os outros recursos do interesse possível incluem:

- Committed Access Rate (CAR)
- Generic Traffic Shaping (GTS)
- Enfileiramento feito sob encomenda

Às vezes, você puder configurar estas características quando sob um ataque ativo.

O CSS pode reduzir o impacto dos ataques de inundação de SYN no VIP e nos servidores reais. À revelia, o CSS restringe o número de SYN e de cumprimentos de três vias incompletos e registra-os como ataques DoS.

Refira a informação de Referência de Segurança para mais informação.

Serviços possivelmente desnecessários

Em regra geral, desabilite todo o serviço desnecessário em qualquer roteador que for alcançável de uma rede potencialmente hostil. Os serviços que esta seção alista são às vezes úteis. Mas desabilite estes serviços se não estão no uso ativo.

SNTP

O SNTP não é especialmente perigoso, mas todo o serviço desnecessário pode apresentar um trajeto para a penetração. Se você usa realmente o SNTP, seja certo configurar explicitamente o origem de tempo confiado. O SNTP não usa a autenticação. Uma corrupção da base de tempo é uma boa maneira de subverter determinados protocolos de segurança. O melhor método é usar uma fonte que seja interna e menos provável ser falsificado.

Protocolo Cisco Discovery

O Cisco Discovery Protocol (CDP), que foi introduzido em WebNS 5.10, é usado para algumas funções de gerenciamento de rede. O CDP é perigoso porque todo o sistema em um segmento diretamente conectado pode executar estas ações:

- Aprenda que o roteador é um dispositivo Cisco
- Determine o número de modelo e a versão de software que corridas

Um atacante pode usar esta informação a fim projetar ataques contra o CSS. As informações de CDP estão acessíveis apenas para sistemas diretamente conectados. O CSS anuncia somente a informação de CDP. O CSS não escuta. Você pode emitir o comando global configuration do **no cdp run** a fim desabilitar o protocolo de CDP. Você não pode desabilitar o CDP no CSS em uma base da interface per.

Estada atualizada

Como todo o software, o software webns de Cisco tem erros. Alguns destes erros têm implicações de segurança. Além, os ataques novos continuam a ser inventados. E o comportamento que foi considerado correto quando uma parte de software foi escrita pode ter efeitos ruim quando o comportamento é explorado deliberadamente.

Quando uma nova e importante vulnerabilidade de segurança é encontrada em um produto Cisco, a Cisco geralmente emite uma nota de aviso sobre a vulnerabilidade. Refira a política da vulnerabilidade de segurança para obter informações sobre do processo com que estas observações são emitidas. Refira Recomendações de Segurança para as observações.

Quase todo o comportamento inesperado de qualquer parte de software pode criar uma exposição de segurança em algum lugar. Erros da menção dos relatórios formais somente que têm implicações diretas para a segurança de sistema. Você pode aumentar sua Segurança se você mantém seu software atualizado, mesmo na ausência de toda a Recomendação de Segurança.

Alguns problemas de segurança não são o resultado dos Bug de Software, e os administradores de rede devem ficar cientes das tendências nos ataques. Há um número Web site, listas de envio de Internet, e de grupos de usuário usenet que são estados relacionados com estas tendências.

Informações Relacionadas

- RFC 2267
- Recomendações de Segurança
- Política da vulnerabilidade de segurança
- Informações de referência de segurança
- Configurando protocolos de rede CSS
- Configurando métodos do Acesso remoto CSS
- Configurando perfis de usuário e Parâmetros CSS
- Notas de versão
- Caracterizando e Rastreando Inundações de Pacote com Uso de Cisco Routers
- ISP Cisco essenciais - Os IO essenciais caracterizam cada ISP devem considerar
- O mais atrasado no ataque de recusa de serviço: Descrição e informação de “Smurf” para minimizar efeitos
- Suporte Técnico e Documentação - Cisco Systems