Technote no FAQ para o Acesso remoto em Cisco ESA/WSA/SMA

Índice

Introdução

Este documento dá respostas às perguntas mais frequentes sobre o uso do Acesso remoto pelo Suporte técnico de Cisco em ferramentas de segurança do índice de Cisco. Isto inclui a ferramenta de segurança do email de Cisco (ESA), a ferramenta de segurança da Web de Cisco (WSA), e o dispositivo do Gerenciamento do Cisco Security (S A).

Pré-requisitos

Componentes Utilizados

A informação neste documento é baseada nas ferramentas de segurança do índice de Cisco que executam toda a versão de AsyncOS.

Que é Acesso remoto?

O Acesso remoto é uma conexão do Shell Seguro (ssh) que seja permitida de uma ferramenta de segurança do índice de Cisco a um host seguro em Cisco. Somente o auxílio do cliente Cisco pode alcançar o dispositivo uma vez que uma sessão remota é permitida. O Acesso remoto permite que o apoio de cliente Cisco analise um dispositivo. O apoio alcança o dispositivo

através de um túnel SSH que este procedimento crie entre o dispositivo e o server de upgrades.ironport.com.

Como o Acesso remoto trabalha

Quando os novatos de uma conexão de acesso remoto, o dispositivo abrirem um seguro, aleatório, porta da alto-fonte através de uma conexão de SSH no dispositivo ao configurado/porta selecionada uma dos seguintes servidores de segurança do índice de Cisco:

IP Address	Hostname	Use
63.251.108.107	upgrades.ironport.com	Todas as ferramentas de segurança satisfeitas
63.251.108.107	c.tunnels.ironport.com	Dispositivos da série C (ESA)
63.251.108.107	x.tunnels.ironport.com	Dispositivos das X-séries (ESA)
63.251.108.107	m.tunnels.ironport.com	Dispositivos das M-séries (S A)
63.251.108.107	s.tunnels.ironport.com	Dispositivos da série S (WSA)

Éimportante notar que um Firewall do cliente pode precisar de ser configurado para permitir acima conexões externas a um dos server listados. Se seu Firewall tem a inspeção do protocolo S TP permitida, o túnel não estabelecerá. As portas que Cisco aceitará conexões do dispositivo para o Acesso remoto são:

- 22
- 25 (padrão)
- 53
- 80
- 443
- 4766

A conexão de acesso remoto é feita a um nome de host e não a um endereço IP de Um ou Mais Servidores Cisco ICM NT duro-codificado. Isto exige o Domain Name Server (DNS) ser configurado no dispositivo a fim estabelecer a conexão externa.

Em uma rede cliente, alguns dispositivos de rede protocolo-cientes podem obstruir este conexão devido à má combinação da /porta do protocolo. Algum protocolo simple mail transport (S TP) - dispositivos cientes pode igualmente interromper a conexão. Nos casos onde há os dispositivos ou as conexões externas protocolo-cientes que são obstruídos, o uso de uma porta a não ser o padrão (25) pode ser exigido. O acesso à extremidade remota do túnel é restringido somente ao apoio de cliente Cisco. Seja por favor certo que você revê seus Firewall/rede para conexões externas ao tentar estabelecer ou pesquisar defeitos conexões de acesso remoto para seu dispositivo.

> **Note**: Quando um engenheiro de suporte do cliente Cisco é conectado ao dispositivo através do Acesso remoto a alerta do sistema no dispositivo mostra *(SERVIÇO)*.

Como permitir o Acesso remoto

> **Note**: Seja por favor certo rever o Guia do Usuário de seu dispositivo e a versão de AsyncOS para instruções em “permitir o Acesso remoto para pessoais de suporte técnico de Cisco”.

Note: Os acessórios enviados através do email a attach@cisco.com não podem ser seguros no trânsito. O gerente do caso de suporte é a opção segura preferida de Cisco transferir arquivos pela rede a informação a seu caso. Para aprender mais sobre a Segurança e as limitações de tamanho de outras opções do upload de arquivo: Uploads de arquivo do cliente ao centro de assistência técnica da Cisco

Identifique uma porta que possa ser alcançada do Internet. O padrão é a porta 25, que trabalhará na maioria de ambientes porque o sistema igualmente exige o acesso geral sobre essa porta a fim enviar mensagens de Email. As conexões sobre esta porta são permitidas na maioria de configurações de firewall.

CLI

A fim estabelecer uma conexão de acesso remoto através do CLI, como um usuário admin, termina estas etapas:

1. Incorpore o comando do **techsupport**
2. Escolha o **TÚNEL**
3. Escolha gerar ou *entrar em uma* corda aleatória da semente
4. Especifique o número de porta para a conexão
5. Responda "**Y**" para permitir o acesso do serviço

O Acesso remoto será permitido neste tempo. O dispositivo trabalha agora para estabelecer a conexão segura ao bastion host seguro em Cisco. Forneça o número de série do dispositivo e a corda da semente que é gerada ao coordenador TAC que apoia seu caso.

GUI

A fim estabelecer uma conexão de acesso remoto através do GUI, como um usuário admin, termina estas etapas:

1. Navegue **para ajudar e o apoio > o Acesso remoto** (para o ESA, o S A), **apoiam e ajuda > Acesso remoto** (para WSA)
2. O clique **permite**
3. Escolha o método para a corda da semente
4. Assegure-se de que você verifique a *conexão iniciada através da* caixa de verificação do *túnel seguro* e especifique o número de porta para a conexão
5. O clique **submete-se**

O Acesso remoto será permitido neste tempo. O dispositivo trabalha agora para estabelecer a conexão segura ao bastion host seguro em Cisco. Forneça o número de série do dispositivo e a corda da semente que é gerada ao coordenador TAC que apoia seu caso.

Como desabilitar o Acesso remoto

CLI

1. Incorpore o comando do **techsupport**
2. Escolha o **DESABILITAÇÃO**
3. Responda "**Y**" quando alertado "é você certo você quer desabilitar o acesso do serviço?"

GUI

1. Navegue **para ajudar e o apoio > o Acesso remoto** (para o ESA, o S A), **apoiam e ajuda > Acesso remoto** (para WSA).
2. **Desabilitação do** clique
3. A saída GUI mostrará o “sucesso — o Acesso remoto foi desabilitado”

Como testar a Conectividade do Acesso remoto

Use este exemplo a fim executar um teste inicial para a Conectividade de seu dispositivo a Cisco:

```
example.run> > telnet upgrades.ironport.com 25

Trying 63.251.108.107...
Connected to 63.251.108.107.
Escape character is '^]'.
SSH-2.0-OpenSSH_6.2 CiscoTunnels1
```

A Conectividade pode ser testada para algumas das portas alistadas acima: 22, 25, 53, 80, 443, ou 4766. Se a Conectividade falha, você pode precisar de executar uma captura de pacote de informação para ver onde a conexão está falhando de seus dispositivo/rede.

Por que o Acesso remoto não trabalha no S A?

O Acesso remoto não pode permitir em um S A se o S A é colocado na rede local sem o de acesso direto ao Internet. Para este exemplo, o Acesso remoto pode ser permitido em um ESA ou em um WSA, e o acesso SSH pode ser permitido no S A. Isto permite o apoio de Cisco a primeiramente conecta através do Acesso remoto ao ESA/WSA, e então do ESA/WSA ao S A através do SSH. Isto exigirá a Conectividade entre o ESA/WSA e o S A na porta 22.

> **Note**: Seja por favor certo rever o Guia do Usuário de seu dispositivo e a versão de AsyncOS para instruções em “permitir o Acesso remoto aos dispositivos sem uma conexão com o Internet direta”.

CLI

A fim estabelecer uma conexão de acesso remoto através do CLI, como um usuário admin, termina estas etapas:

1. Incorpore o comando do **techsupport**
2. Escolha **SSHACCESS**
3. Escolha gerar ou *entrar em uma* corda aleatória da semente
4. Responda “**Y**” para permitir o acesso do serviço

O Acesso remoto será permitido neste tempo. A saída CLI mostrará a corda da semente. Forneça por favor isto ao engenheiro de suporte do cliente Cisco. A saída CLI igualmente mostrará os detalhes do status de conexão e do Acesso remoto, incluindo o número de série do dispositivo. Forneça por favor este número de série ao engenheiro de suporte ao cliente do cliente.

GUI

A fim estabelecer uma conexão de acesso remoto através do GUI, como um usuário admin, termina estas etapas:

1. Navegue **para ajudar e o apoio > o Acesso remoto** (para o ESA, o S A), **apoiam e ajuda > Acesso remoto** (para WSA)
2. O clique **permite**
3. Escolha o método para a corda da semente
4. Não verifique a *conexão iniciada através da* caixa de verificação do *túnel seguro*
5. O clique **submete-se**

O Acesso remoto será permitido neste tempo. A saída GUI mostrar-lhe-á um mensagem de sucesso e a corda da semente do dispositivo. Forneça por favor isto ao engenheiro de suporte do cliente Cisco. A saída GUI igualmente mostrará o status de conexão e os detalhes do Acesso remoto, incluindo o número de série do dispositivo. Forneça por favor este número de série ao engenheiro de suporte ao cliente do cliente.

Como desabilitar o Acesso remoto quando permitido para SSHACCESS

O Acesso remoto de desabilitação para SSHACCESS é as mesmas etapas da maneira prevista acima.

Troubleshooting

Se o dispositivo não é Acesso remoto permitido capaz e conecta a upgrades.ironport.com através de uma das portas alistadas, você precisará de executar uma captura de pacote de informação diretamente do dispositivo para rever o que está fazendo com que a conexão externa falhasse.

> **Note**: Seja por favor certo rever o Guia do Usuário de seu dispositivo e a versão de AsyncOS para instruções em “executar uma captura de pacote de informação”.

O engenheiro de suporte do cliente Cisco pode pedir para ter o arquivo .pcap fornecido a fim rever e ajudar com Troubleshooting.

Informações Relacionadas

- ESA FAQ: Que são os níveis do acesso administrativo disponíveis no ESA?
- Cisco envia por correio eletrónico a sustentação do produto da ferramenta de segurança
- Apoio de produtos de segurança da Web de Cisco
- Sustentação do produto do dispositivo do Gerenciamento de segurança do índice de Cisco
- Suporte Técnico e Documentação - Cisco Systems