Guia de Design da ferramenta de segurança da Web

Índice

Introdução

Este documento descreve como projetar a ferramenta de segurança da Web de Cisco (WSA) e componentes associados para o desempenho ótimo.

Informações de Apoio

Quando você projeta uma solução para o WSA, exige a consideração cuidadosa, não somente com respeito à configuração do dispositivo própria, mas igualmente os dispositivos de rede associados e suas características. Cada rede é uma Colaboração dos dispositivos múltiplos, e se um deles não participa corretamente na rede, a seguir do usuário que as experiências puderam diminuir.

Há dois componentes principais que devem ser considerados quando você configura o WSA: o hardware e o software. O hardware vem em dois tipos diferentes. O primeiro é o tipo físico de hardware, tal como os modelos S170, S380, e de S680 Series, assim como a outra extremidade de modelos da vida (EoL), tais como os modelos S160, S360, S660, S370, e de S670 Series. O outro tipo de hardware é virtual, como os modelos da série S000v, S100v, e S300v. O operating system (OS) que é executado neste hardware é chamado *AsyncOS para a Web*, que é baseada no FreeBSD em seu núcleo.

O WSA oferece o serviço de proxy e também faz a varredura, inspeciona, e categoriza de todo o tráfego (HTTP, HTTPS, e File Transfer Protocol (FTP)). Toda a corrida destes protocolos sobre o TCP e confia pesadamente no Domain Name System (DNS) para a operação apropriada. Por

estas razões, a saúde de rede é vital para a operação apropriada do dispositivo e a sua comunicação com as várias partes da rede, tanto dentro como fora do controle da empresa.

Projeto

Use a informação que é descrita nesta seção a fim projetar o WSA e os componentes relativos para o desempenho ótimo.

Rede

Uma rede sem erros, rápida é vital para a operação apropriada do WSA. Se a rede é instável, a experiência do usuário pôde diminuir. Os problemas de rede geralmente são detectados quando os página da web tomam mais por muito tempo para alcançar ou são inacessíveis. A inclinação inicial é culpa o dispositivo, mas é geralmente a rede que se porta mal. Assim, a consideração cuidadosa e a auditoria devem ser feitas a fim assegurar-se de que a rede ofereça o melhor serviço para protocolos do aplicativo de nível elevado tais como o HTTP, o HTTPS, o FTP, e o DNS.

Considerações gerais

Estão aqui algumas considerações gerais que você pode executar a fim assegurar o melhor comportamento de rede:

- Assegure-se de que a rede da camada 2 (L2) esteja estável, que a operação da medir-árvore está correta, e que não há umas computações e umas alterações de topologia frequentes da medir-árvore.
- O protocolo de roteamento que é usado deve igualmente fornecer a convergência rápida e a estabilidade. Os temporizadores rápidos do Open Shortest Path First (OSPF) ou o Enhanced Interior Gateway Routing Protocol (EIGRP) são boas escolhas para tal rede.
- Use sempre pelo menos duas interfaces de dados no WSA: um que enfrenta os computadores do utilizador final, e outro para a operação de partida (conectada ao proxy upstream ou ao Internet). Isto está feito a fim eliminar o recurso possível força, como quando o número de portas TCP é esgotado ou quando os bufferes da rede se tornam completamente (com o uso do interfaces únicas para tanto dentro como fora de especialmente).
- Dedique a interface de gerenciamento para o tráfego do Gerenciamento-somente a fim aumentar a Segurança. A fim conseguir isto através do GUI, navegar à **rede > às relações** e verificar a caixa de verificação **separada do roteamento (porta M1 restringida aos serviços da gerência do dispositivo somente)**.
- Use servidores DNS rápidos. Toda a transação através do WSA exige pelo menos uma pesquisa de DNS (se não no esconderijo). Um servidor DNS que seja lento ou se porte mal influências toda a transação e seja observado como a conectividade de Internet atrasada ou

lenta.

- Quando as tabelas de roteamento separadas são usadas, estas regras aplicam-se:

  Todas as relações são incluídas na tabela de roteamento do *Gerenciamento do* padrão (M1, P1, P2).

  Somente as interfaces de dados são incluídas na tabela de roteamento dos *dados*.

  Note: A separação de tabelas de roteamento é não pela relação, mas um pouco pelo serviço. Por exemplo, o tráfego entre o WSA e o controlador de domínio do microsoft ative directory (AD) obedece sempre as rotas que são especificadas na tabela de roteamento do Gerenciamento, e é possível configurar as rotas que indicam da relação P1/P2 nesta tabela. Não é possível incluir as rotas na tabela de roteamento dos dados que usam as interfaces de gerenciamento.

Balanceamento de carga

Estão aqui algumas considerações da função de balanceamento de carga que você pode executar a fim assegurar o melhor comportamento de rede:

- O do do â da rotação DNS isto é o termo usado quando um único hostname é usado como um proxy, mas tem registros do múltiplo A no servidor DNS. Cada cliente resolve este a um endereço IP de Um ou Mais Servidores Cisco ICM NT diferente e usa proxys diferentes. Uma limitação é que as mudanças de registros DNS estão refletidas em clientes em cima da repartição (DNS local que põe em esconderijo), assim que oferece um nível baixo do vigor se uma mudança deve ser feita. Contudo, isto é transparente aos utilizadores finais.

- O do do â dos arquivos do controle de endereço de proxy (PAC) estes é os arquivos proxy-automáticos do script que determinam como cada URL deve ser segurada em um navegador baseado nas funções escritas dentro dela. Tem a característica para enviar a mesma URL sempre diretamente ou ao mesmo proxy.

- O do do â da descoberta automática isto descreve o uso de métodos DNS/DHCP a fim obter os arquivos PAC (descritos na consideração precedente). Geralmente, estas primeiras três considerações são combinadas em uma solução. Contudo, isto pode ser complicado e muitos agentes de usuário, tais como o microsoft office, descargador de Adobe, Javascript, e flash, não podem ler arquivos PAC de todo.

- O do do â do protocolo web cache control (WCCP) este protocolo (especialmente versão de WCCP 2) fornece um robusto e muito uma maneira eficiente criar a função de balanceamento de carga entre diversos WSAs e para incorporar igualmente a Alta disponibilidade.

- O separado Cisco do do â dos dispositivos da função de balanceamento de carga recomenda que você usa os carga-equilibradores como máquinas dedicadas.

Firewall

Estão aqui algumas considerações do Firewall que você pode executar a fim assegurar o melhor comportamento de rede:

- Assegure-se de que o Internet Control Message Protocol (ICMP) esteja permitido durante todo a rede de cada fonte. Isto é vital, porque o WSA depende do mecanismo de descoberta máximo da unidade da transição do trajeto (MTU), como descrito no RFC 1191, que depende das requisições de eco ICMP (tipo 8) e respostas de eco (tipo 0), e a inacessível-fragmentação ICMP é exigida (tipo 3, código 4). Se você desabilita o Path MTU Discovery no WSA com o comando CLI do **pathmtudiscovery**, a seguir o WSA usa o MTU padrão de 576 bytes, conforme o RFC 879. Isto impacta o desempenho devido às despesas gerais aumentadas e uma remontagem dos pacotes.

- Assegure-se de que não haja nenhum roteamento assimétrico dentro da rede. Quando este não for um problema no WSA, todo o Firewall que for encontrado ao longo do trajeto deixa cair os pacotes porque não recebeu ambos os lados da comunicação.

- Com Firewall, é muito importante excluir os endereços IP de Um ou Mais Servidores Cisco ICM NT WSA das ameaças como estações regulares do computador da extremidade. O Firewall pôde pôr os endereços IP de Um ou Mais Servidores Cisco ICM NT WSA devido a conexões demais (conforme o conhecimento geral do Firewall).

- Se o Network Address Translation (NAT) é empregado para qualquer endereço IP de Um ou Mais Servidores Cisco ICM NT WSA no dispositivo das premissas do cliente, assegure-se de que cada WSA use um endereço global externo separado no NAT. Se você usa o NAT para WSAs múltiplo que tem um único endereço global externo, você pôde encontrar estas edições:

  Todas as conexões de todo o WSAs ao mundo exterior usam um único endereço global externo, e o Firewall é executado rapidamente fora dos recursos.

  Se há um ponto do tráfego para esse destino único, o servidor de destino pôde pôr o e eliminar a empresa inteira do acesso a este recurso. Este pôde ser um recurso valioso como o armazenamento da nuvem da empresa, as conexões da nuvem do escritório, ou as atualizações de antivírus do por-computador.

Identidades

Recorde que o *lógico E o* princípio se aplicam em todos os componentes da identidade. Por exemplo, se você configura o agente de usuário e o endereço IP de Um ou Mais Servidores Cisco ICM NT, significa o agente de usuário deste endereço IP de Um ou Mais Servidores Cisco ICM NT. Não significa o agente de usuário *ou* este endereço IP de Um ou Mais Servidores Cisco ICM NT.

Use uma identidade para a autenticação do mesmo tipo substituto (ou de nenhum substituto) e/ou de agente de usuário.

Éimportante assegurar-se de que cada identidade que exige a autenticação inclua as cordas do agente de usuário para os navegadores/agentes de usuário que apoiam a autenticação de proxy, tal como o internet explorer, Mozilla Firefox, e Google Chrome conhecidos. Há alguns aplicativos

que exigem o acesso ao Internet mas não apoia a autenticação proxy/WWW.

As identidades são de cima para baixo combinado com a busca para fósforos que termina na primeira entrada combinada. Por este motivo, se você tem a *identidade 1* e a *identidade 2* configurada, e uma identidade 1 dos fósforos da transação, não se verifica contra a identidade 2.

Acesso/descriptografia/roteamento/políticas de partida do malware

Estas políticas são aplicadas contra tipos de tráfego diferentes:

- As políticas de acesso são aplicadas contra o HTTP liso ou as conexões de FTP. Determinam se a transação deve ser aceitada ou deixado cair.

- As políticas de descriptografia determinam se as transações HTTPS devem ser decifradas, deixado cair, ou passado completamente. Se a transação é decifrada, a seguir o consecutivo parte de pode-se ver como um pedido do HTTP liso e está combinado contra políticas de acesso. Se você deve deixar cair um pedido HTTPS, deixe-o cair nas políticas de descriptografia, não nas políticas de acesso. Se não, consome mais CPU e memória para uma transação deixada cair primeiramente a ser decifrada e a ser deixada cair então.

- As políticas de roteamento determinam a direção de upstream de uma transação uma vez que ele que o seu permitiu com o WSA. Isto aplica se há uns proxys upstream ou se o WSA reage do modo do *conector* e envia o tráfego à torre da Segurança da Web da nuvem.

- As políticas de partida do malware são aplicadas contra transferências de arquivo pela rede HTTP ou FTP dos utilizadores finais para servidores de Web. Isto é visto geralmente é um pedido do cargo HTTP.

Para cada tipo de política, é importante recordar que o *lógico OU o* princípio se aplicam. Se você tem identidades múltiplas consultadas, a seguir a transação deve combinar algumas das identidades que são configuradas.

Para um controle mais granulado, use estas políticas. As identidades errada configuradas pela política podem criar as edições, onde é mais benéfico usar diversas identidades providas em uma política. Recorde que identidades não impactam o tráfego, apenas identificam os tipos de tráfego para uns fósforos mais atrasados em uma política.

Frequentemente épocas, as políticas de descriptografia usam identidades com autenticação. Quando isto não for errado e é precisado às vezes, o uso de uma identidade com a autenticação provida na política de descriptografia significa que todas as transações que combinam a política de descriptografia estão decifradas para que a autenticação ocorra. A ação da descriptografia pôde ser deixada cair ou passado completamente, mas desde que há uma identidade com autenticação, a descriptografia ocorre a fim deixar cair ou passar mais tarde com o tráfego. Isto é caro e deve ser evitado.

Algumas configurações foram observadas que contêm 30 ou mais identidades e 30 ou mais políticas de acesso, onde todas as políticas de acesso incluem todas as identidades. Neste caso, não há nenhuma necessidade de usar este muitas identidades se são combinadas em todas as políticas de acesso. Quando isto não prejudicar a operação do dispositivo, cria a confusão com as tentativas de pesquisar defeitos e é caro com respeito ao desempenho.

Categorias feitas sob encomenda URL

O uso de categorias feitas sob encomenda URL é uma ferramenta poderosa no WSA que geralmente é entendido mal e empregado mal. Por exemplo, há as configurações que contêm todos os locais video para fósforos na identidade. O WSA tem uma ferramenta incorporado que automaticamente atualizações quando os locais video mudam URL, que ocorre frequentemente. Assim, faz o sentido permitir que o WSA controle as categorias URL automaticamente, e usa as categorias do costume URL para locais especiais, não ainda categorizados.

Seja muito cuidadoso com expressões regulares. Se os fósforos do caractere especial tais como o ponto (.) e a estrela (*) são usados, puderam provar ser muito CPU e memória extensivos. O WSA expande toda a expressão regular para combiná-la contra cada transação. Por exemplo, está aqui uma expressão regular:

```
example.*
```

Esta expressão combinará toda a URL que contiver o *exemplo da* palavra, não somente o domínio de *example.com*. Evite o uso do *ponto* e *protagonizar em* expressões regulares e use-as somente como um último recurso.

Está aqui um outro exemplo de uma expressão regular que possa criar edições:

```
www.example.com
```

Se você usa este exemplo nas expressões regulares arquivado, combinará não somente *www.example.com*, mas igualmente *www.www3example2com.com*, como o ponto aqui significa todo o *caráter*. Se você deseja combinar somente *www.example.com*, escape o ponto:

```
www\.example\.com
```

Neste caso, não há nenhuma razão usar a característica das expressões regulares quando você pode incluir este dentro do domínio da categoria do costume URL com este formato:

```
www.example.com
```

Anti-malware e reputação

Se mais de um motor de varredura é permitido, considere a opção permitir a varredura adaptável igualmente. A exploração adaptável é um motor poderoso mas pequeno no WSA que as pré-varreduras cada pedido e determinam o motor detalhado que deve ser pedidos de varredura usados. Isto aumenta levemente o desempenho no WSA.