Práticas recomendadas de agendamento de atualização de conteúdo de firewall seguro

Problema

As empresas que gerenciam dispositivos FTD (Firewall Threat Defense, defesa contra ameaças de firewall) com FMC (Firewall Management Center, centro de gerenciamento de firewall) exigem orientação sobre as práticas recomendadas para aplicar atualizações de segurança e conteúdo. Especificamente, há uma incerteza sobre a frequência com que os diferentes tipos de atualização devem ser aplicados, se as atualizações podem ser agendadas em vez de aplicadas imediatamente e quais são os impactos operacionais dessas atualizações. A pergunta surge porque a Cisco lança atualizações de conteúdo com frequência, às vezes semanalmente, e os administradores precisam entender se elas devem ser aplicadas imediatamente após o lançamento ou se podem ser programadas de acordo com janelas de manutenção organizacional e políticas de gerenciamento de alterações.

Ambiente

- Cisco Secure Firewall Firepower, todas as versões
- Firepower Management Center, todas as versões

Resolução

Esta tabela mostra a finalidade de cada tipo de atualização no Firepower.

Tipo de atualização	Propósito	Notas
SRU/LSP	Atualizações de regra de intrusão (Snort 2 e Snort 3, respectivamente)	Mantém as regras de detecção/prevenção de intrusão

GeoDB	Dados de geolocalização para endereços IP	Usado para filtragem de tráfego baseada em geolocalização
VDB	Informações de vulnerabilidade e impressões digitais de host	Usado para avaliação de vulnerabilidade e análise de risco

As atualizações de conteúdo do Cisco Secure Firewall são categorizadas em três tipos distintos, cada um com frequências de lançamento diferentes e práticas de programação recomendadas. Esta tabela descreve as práticas recomendadas de programação para cada tipo de atualização:

Tipo de atualização	Frequência de Liberação	Programação Sugerida	Agenda FMC padrão	Caminho de Navegação (a Ser Modificado)
SRU/LSP	Frequente	Diariamente	Diariamente	Sistema > Atualizações de Conteúdo > Atualizações de Regra
GeoDB	~Semanalmente	Semanalmente	Semanalmente	Sistema > Atualizações de Conteúdo > Atualizações de Geolocalização
VDB	~Mensal	Semanalmente	Semanalmente	Sistema > Ferramentas: Agendamento > Download semanal de software

Para configurações e postura de segurança ideais, a prática recomendada é aplicar qualquer uma dessas atualizações assim que elas forem lançadas pela Cisco. Alguns desses arquivos de atualização podem ser razoavelmente grandes e as alocações de largura de banda precisam ser consideradas. É recomendável instalar as atualizações maiores fora dos horários de pico de tráfego, se estiver usando a mesma rede.

Atualizações de SRU/LSP (regras de intrusão)

As atualizações de regras do Snort (SRU) e os Lightweight Security Packages (LSP) contêm regras de detecção e prevenção de intrusão. Essas atualizações devem ser aplicadas com a frequência operacionalmente possível para manter a proteção contra ameaças emergentes.

Para modificar a programação SRU/LSP: Navegue para System > Content Updates > Rule Updates na interface do FMC para ajustar as configurações de hora, data e frequência.

As atualizações de SRU/LSP suportam implantação automatizada e podem ser programadas para implantação automática após o download e a instalação.

Atualizações do GeoDB (Banco de Dados de Geolocalização)

As atualizações do banco de dados de geolocalização fornecem dados atuais de localização geográfica para endereços IP e geralmente são liberadas semanalmente.

Para modificar o agendamento do GeoDB: Navegue para System > Content Updates > Geolocation Updates na interface do FMC para ajustar os parâmetros de agendamento.

As atualizações do GeoDB podem ser programadas para download e instalação, mas a implantação em dispositivos gerenciados requer envio manual e não pode ser totalmente automatizada como atualizações SRU/LSP.

Atualizações do VDB (Vulnerability Database, banco de dados de vulnerabilidade)

As atualizações do banco de dados de vulnerabilidades são lançadas aproximadamente mensalmente e gerenciadas como atualizações de software, em vez de atualizações de conteúdo.

Para modificar o agendamento do VDB: Navegue até Sistema > Ferramentas: Agendamento e modificação da tarefa de Download semanal de software para ajustar a frequência e o tempo de download.

As atualizações de VDB se enquadram nas atualizações de software e não podem ser implantadas independentemente. Elas são incluídas ao executar implantações manuais que compilam todas as alterações pendentes.

Considerações de implantação

Ao implantar atualizações, o FMC compila todas as alterações de configuração pendentes e pode incluir vários tipos de atualizações de conteúdo em uma única operação de implantação. Algumas atualizações podem causar breves reinicializações do serviço Snort durante a implantação, o que deve ser considerado ao agendar atualizações durante o horário de produção.

As empresas devem alinhar os agendamentos de atualizações com suas políticas de gerenciamento de alterações e considerar o agendamento de atualizações durante as janelas de manutenção se interrupções breves do serviço forem uma preocupação para seu ambiente

operacional.

Causa

Tratava-se de uma solicitação de orientação operacional e de configuração, e não de um defeito técnico. A necessidade de esclarecimento surgiu da incerteza sobre as práticas de agendamento de atualização, os recursos de automação e o impacto operacional de diferentes tipos de atualização de conteúdo em ambientes Cisco Secure Firewall.

Conteúdo relacionado

- Guia de Administração do Cisco Secure Firewall Management Center, 7.6: Atualizações
- Suporte técnico e downloads da Cisco

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.