Evite a Inatividade de Rede com a Solução de Alta Disponibilidade para o WatchGuard Firebox

A Inatividade Pode Ser Desastrosa

A inatividade de rede custa caro para empresas de todos os tipos e tamanhos. Falhas na rede de TI da empresa podem levar a prejuízos devido a atrasos em fluxos de trabalho essenciais, como produção, comunicação, processamento de pedidos, transferência de arquivos, contas a pagar e a receber, relatórios e muito mais.

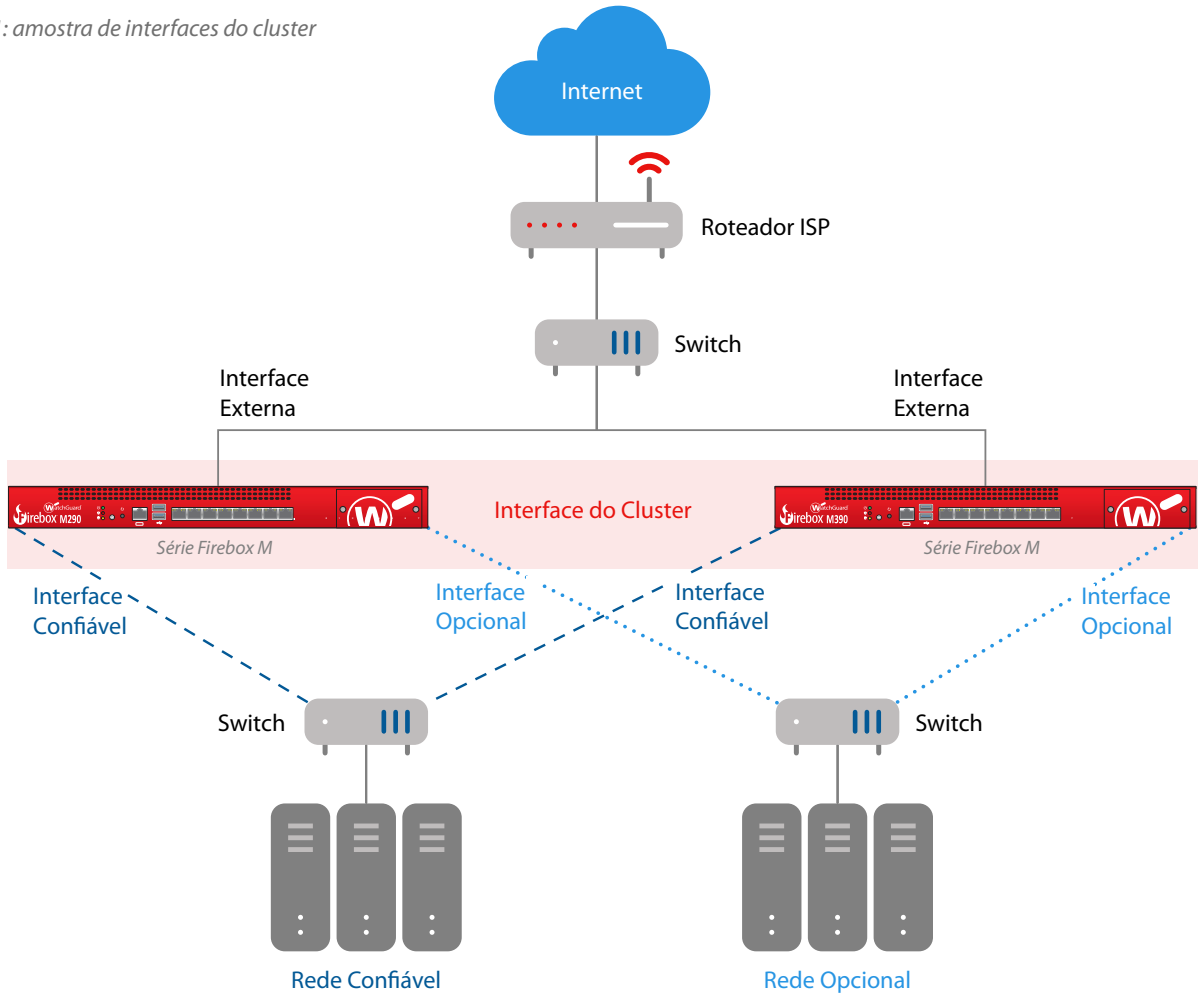
Nenhum recurso na topologia de segurança de rede faz mais para proteger a continuidade dos negócios e prevenir atrasos prejudiciais do que implementar appliances de segurança de alta disponibilidade.

A Solução da WatchGuard®: FireCluster

Para aumentar a escalabilidade e o desempenho de rede, configure o FireCluster, uma solução de alta disponibilidade para os WatchGuard Fireboxes. A alta disponibilidade permite instalar e usar dois firewalls em uma configuração de failover, além de oferecer a redundância necessária para garantir o tempo máximo de atividade da rede. Usar um cluster significa conectar dois dispositivos para que funcionem como uma única unidade lógica, obtendo maior potência de processamento e facilidade de uso.

O FireCluster da WatchGuard, uma função inovadora de cluster de alta disponibilidade, é um componente do sistema operacional Fireware. Ele permite que uma empresa adicione um appliance de segurança de rede idêntico para obter escalabilidade e redundância. Ao ativar o FireCluster, você pode gerenciar e monitorar os dois dispositivos no cluster, como se fossem um único.

Figura 1: amostra de interfaces do cluster

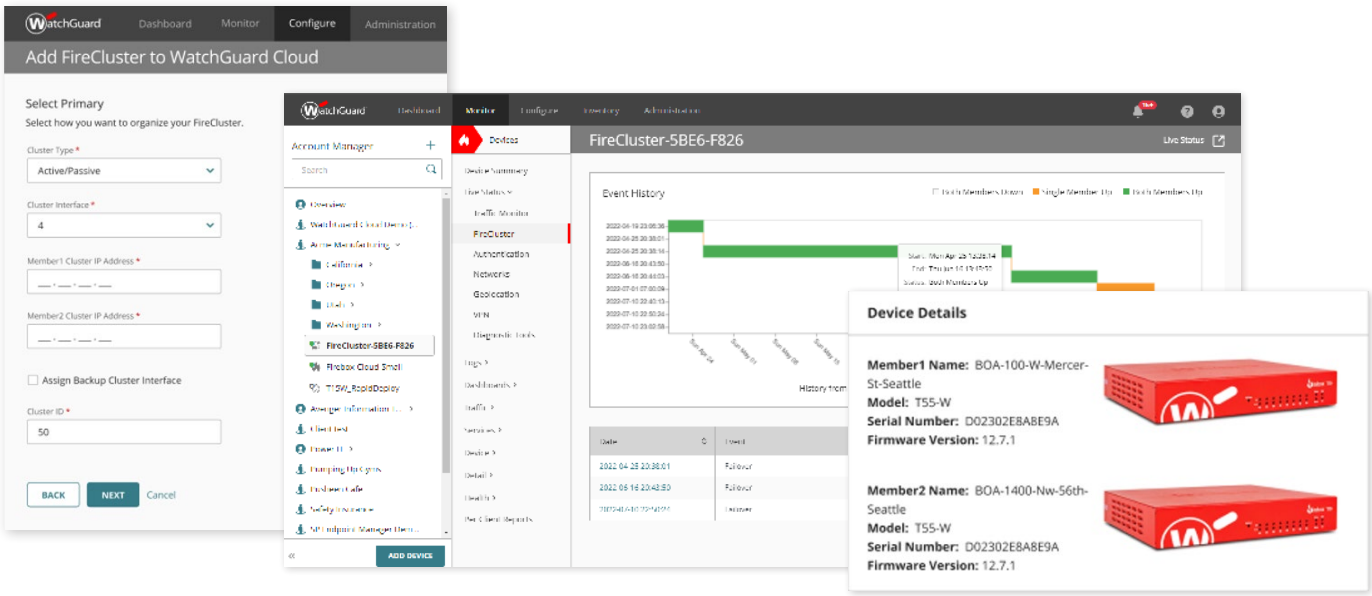


Visão Geral do FireCluster

Sobre o FireCluster

O FireCluster pode ser configurado de duas formas: redundância (ativo/passivo) ou compartilhamento de carga e escalabilidade (ativo/ativo). O monitoramento e os registros do FireCluster concedem ao administrador a visibilidade e o controle necessários para gerenciar o cluster sem sobrecarregar as atividades de rotina.

Figura 2:



Cluster Ativo/Passivo

Em um cluster ativo/passivo, um membro do cluster é ativo e o outro é passivo. O membro ativo lidará com todo o tráfego da rede, a menos que ocorra um evento de failover. O membro passivo monitora ativamente o status do dispositivo ativo. Se o dispositivo ativo falhar, o dispositivo passivo enviará um ARP gratuito e assumirá o controle das conexões.

Cluster Ativo/Ativo

Em um cluster ativo/ativo, os membros compartilham o tráfego. Para distribuir as conexões entre os Fireboxes ativos no cluster, configure o FireCluster para usar um algoritmo com menos conexões ou com rodízio. Em caso de falha em um dos dispositivos, o outro realizará as conexões atribuídas ao dispositivo com falha. Em um ambiente de cluster ativo/ativo, o tráfego é distribuído a cada membro do cluster ao mesmo tempo, pois eles compartilham o mesmo endereço virtual MAC (VMAC). Essa opção é menos usada porque requer configuração no switch e a capacidade de carga geral é cortada pela metade se um dos membros falhar.

Funções do Cluster

É essencial entender a função de cada Firebox no cluster. No FireCluster, um dispositivo é o cluster principal e o outro é o backup principal. O backup principal usa a interface do cluster primário para sincronizar as informações de conexão e sessão com o cluster principal. Se a interface do cluster primário falhar ou se desconectar, o backup principal usará a interface de backup para se comunicar com o cluster principal. O administrador de TI precisa configurar a interface do cluster primário e do cluster de backup para garantir que, caso ocorra um failover no cluster principal, o backup tenha todas as informações necessárias para se tornar o cluster central e transferir conexões e sessões de forma adequada.

Cluster Principal

Esse cluster atribui os fluxos do tráfego da rede e responde a todas as solicitações de sistemas externos como o WatchGuard System Manager, SNMP, DHCP, ARP, protocolos de roteamento e IKE. As configurações ou alterações feitas no cluster serão salvas no cluster principal, que pode ser qualquer um dos dispositivos. O primeiro cluster a ser ligado será o cluster principal.

Cluster de Backup

Esse membro do cluster sincroniza todas as informações necessárias para se tornar o cluster principal em caso de falha. O cluster de backup pode ser ativo ou passivo.

Membro Ativo

Todos os membros do cluster que lidam ativamente com fluxo de tráfego são membros ativos. Em um cluster ativo/ativo, os dois dispositivos são ativos, enquanto em um cluster ativo/passivo, o cluster principal é o único dispositivo ativo.

Membro Passivo

Um Firebox em um cluster ativo/passivo não lidará com fluxos de tráfego de rede, a menos que um dispositivo ativo falhe. Em um cluster ativo/passivo, o membro inativo é o backup principal.

Eventos de Failover em um FireCluster

Quando ocorre um failover no cluster principal, o backup toma o lugar dele. Em seguida, o cluster principal original reinicia e se torna o cluster de backup. Cada membro mantém constantemente as informações de estado e sessão dos dois tipos de cluster. Quando ocorre um failover, as conexões de filtro de pacotes,
os túneis BOVPN e as sessões dos usuários do dispositivo com falha são transferidos automaticamente para o outro dispositivo do cluster.

Quando um membro falha, o cluster transfere e mantém o seguinte:

- Conexões de filtro de pacotes
- Túneis BOVPN
- Sessões do usuário
- Sessões do usuário do Access Portal

Quando ocorre um evento de failover, estas conexões podem ser desfeitas:

- Conexões de proxy
- Conexões de VPN móveis
- Conexões RDP e SSH iniciadas pelo Portal de Acesso

Observação: Os usuários de VPN móvel podem precisar reiniciar a conexão de forma manual depois de um evento de failover.

Tipo de conexão/sessão	Impacto de um evento de failover
Conexões de filtro de pacotes	As conexões são transferidas para outro membro do cluster.
Túneis BOVPN	Os túneis são transferidos para outro membro do cluster.
Sessões do usuário	As sessões são transferidas para outro membro do cluster.
Conexões de proxy	As conexões atribuídas ao dispositivo com falha (principal ou backup) precisam ser reiniciadas. As conexões atribuídas ao outro dispositivo não são interrompidas.
VPN móvel com IPSec	Se o cluster principal falhar, todas as sessões precisarão ser reiniciadas.
VPN móvel com SSL	Em um evento de failover, é preciso reiniciar todas as sessões.
VPN móvel com PPTP	Todas as sessões PPTP são atribuídas ao cluster principal, mesmo em um cluster ativo/ativo. Se o cluster principal falhar, todas as sessões precisarão ser reiniciadas. Se o backup principal falhar, as sessões PPTP não serão interrompidas.

***Tabela 1**: impacto de um evento de failover do FireCluster*

Modelos Compatíveis com o FireCluster

Para configurar um FireCluster, é necessário possuir dois Fireboxes compatíveis do mesmo modelo. Nos modelos Firebox que são compatíveis com interfaces modulares, é necessário ter o mesmo número e tipo de módulos de interface instalados nos mesmos slots dos dispositivos.

Próximas Etapas

O FireCluster da WatchGuard ajuda as empresas que querem garantir maior tempo de atividade da rede, previsão de desempenho e capacidade.

A WatchGuard tem a maior rede de revendedores de valor agregado e de provedores de serviço do setor. Confira nossa rede de parceiros certificados em https://findpartner.watchguard.com/

Sobre a WatchGuard

A WatchGuard® Technologies, Inc. é líder global em segurança cibernética unificada. A nossa abordagem de Unified Security Platform® foi projetada exclusivamente para que provedores de serviços gerenciados forneçam segurança de alto nível que aumenta a escala e a velocidade de seus negócios e, ao mesmo tempo, melhora a eficiência operacional. Adotados em todo o mundo por mais de 17 mil parceiros de segurança e prestadores de serviços para proteger mais de 250 mil clientes, os premiados produtos e serviços da empresa incluem segurança e inteligência de rede, proteção avançada de endpoint, autenticação multifator e Wi-Fi seguro. Juntos, eles oferecem uma plataforma de segurança com cinco elementos indispensáveis: segurança abrangente, conhecimento compartilhado, clareza e controle, alinhamento operacional e automação. A WatchGuard tem sua sede em Seattle, no estado de Washington, nos EUA, e escritórios na América do Norte, Europa, Ásia-Pacífico e América Latina. Para saber mais, acesse **WatchGuard.com/br**.

Para obter mais informações gerais, de promoções e de atualizações, siga a WatchGuard no Twitter @WatchGuard, no Facebook ou na página do LinkedIn. Acesse também nosso blog de InfoSec, Secplicity, para obter informações em tempo real sobre as ameaças mais recentes e como lidar com elas em **www.secplicity.org**.