DMVPN

Elementos da DMVPN
-IPSEC
-NHRP
-GRE/mGRE
-BGP/OSPF

DMVPN, que permite a implementação de redes virtuais privadas (VPNs) de pequeno, médio ou mesmo de grande porte, de forma simples e rápida, por meio da combinação de tunelamento GRE,
IPSec e NHRP (Next Hop Resolution Protocol).

Solução baseada para construção/configuração de canais seguros utilizando IPSEC mais processo GRE de maneira de maneira dinamica e escalavel.

Somente a referencia elemento central necessita de ip estatico.

no-touch - Ex APIC-EM e Cisco Prime.

O spoke estabelece conexão com o elemento central se autentica fecha o canal seguro e se registra utilizando NHRP no Hub site. Sobe o processo de protocolo GRE e estabelece a vizinhança utilizando
o protocolo de roteamento. Recomendado BGP e EIGRP.

.Next Hop Resolution Protocol (NHRP) – O HUB da topologia mantém uma base de dados com os endereços válidos (públicos / roteáveis) de todos os SPOKES da rede. Informa quem
são os vizinhos.
-Camada 2 (Enlace).

Mapeia a interface tunnel com o ip externo utilizado pelo peer (nbma adress).

.Multipoint GRE Tunnel Interface – Permite que uma única interface GRE suporte múltiplos túneis IPsec.

Os spokes mantém um túnel IPsec permanente com o HUB, porém, não entre eles. Quando um spoke precisa enviar um pacote com destino a outro spoke, ele realiza uma busca na base de dados
NHRP para identificar o endereço público (roteável) do spoke em questão. O túnel entre os spokes é então estabelecido via interface mGRE.

ADVPN (Auto Discovery VPN)

É uma tecnologia que permite ao HUB central informar dinamicamente spokes sobre um caminho melhor para o tráfego entre dois spokes. Quando ambos os spokes reconhecem as informações do
HUB, eles estabelecem um túnel de atalho e mudam a topologia de roteamento para o host para alcançar o outro lado sem enviar tráfego através do HUB.

O ADVPN usa uma extensão do protocolo IKEv2 para trocar mensagens entre dois peers, o que permite que os spokes estabeleçam um túnel de atalho entre si.

GRE - Multicast, Unicast. Pega update de roteamento dinamico para depois ser protegido via IPSEC. Se a interface configurada for somente GRE ela so fecha conexão com o HUB e se ela for
mGRE ela fecha conexão com os vizinhos.

GRE - Protocolo de tunelamento. Minimo overhead.
Usado muito para tunelar anuncio de rotas
Não tem criptografia.
Não necessita de NHRP.

Performace routing - PRv3

É a inteligencia do processo IWAN para fazer o balanceamento da carga atraves dos caminhos conhecidos e de acordo com os criterios de performace requiridos para a rede.
Baseado em aplicações e marcações de QoS.

Domain Controle (DC)
Um por solução, o cara que manda;
Notificado a descoberta dos sites, dos peers, prefixos, quais redes vão fazer parte da solução, as politicas. Poder ser DC+MC.
Ele tem as informações, recebe os reports e passa essas informações entre os MC.

Master Controle (MC)

Mapea os borders e aplica as politicas locais, verifica e reportar para o DC.
Tem como objetivo informar o site local qual qual o caminho a ser seguido.

Border router (BR)
Fazer o encaminhamento de acordo com as informações notificadas. Se não tiver segue a RIB.
Tem a função de medir a qualidade de cada um dos caminhos e enviar para o MC.

AVC
Classificação do trafego de aplicativos usando recursos de QoS.
O agente de monitoramento incorporado do AVC mede os tempos de transação e a latência dos aplicativos TCP. E mede a perda de pacotes e o jitter para aplicativos de voz e vídeo.

-delay - Representa a diferença de tempo entre o envio e o recebimento de um sinal.
-jitter - È uma variação estatística do atraso na entrega de dados em uma rede.
-loss path

sh domain IWAN master traffic-classes summary

BGP

Atributos de caminho
– AS-PATH • SAs que o rota anunciada percorre
• ASN - Autonomous System Number
– Número único para cada SA no mundo
– NEXT-HOP • Interface a ser enviado o pacote
– ORIGIN • Fonte de informações de roteamento

Routing Information Base (RIB)
– O BGP • pressupõe a existência de um iGP
• não possui algoritmos próprios para o cálculo das tabelas de rotas
• importa rotas de outras fontes
– A RIB armazena todas essas rotas
– Políticas de Importação
• Filtram as rotas que irão para a RIB
– Políticas de Exportação
• Filtram as rotas que serão anunciadas pelo BGP

Routing Information Base (RIB)
– Adj-RIBs-In
• Informações de roteamento não editadas recebidas por roteadores vizinhos
– Loc-RIB
• Informações usadas pelo roteador para encaminhamento

• Aplicação das políticas de roteamento
– Adj-RIBs-Out
• Informações que o roteador escolhe para anunciar aos seus vizinhos

O BGP permite o roteamento baseado em políticas. Você pode usar políticas de roteamento para escolher entre vários caminhos para um destino e controlar a redistribuição de informações de roteamento.

O BGP usa o TCP como seu protocolo de transporte, usando a porta 179 para estabelecer conexões. A execução de um protocolo de transporte confiável elimina a necessidade de o BGP implementar a fragmentação, a retransmissão, a confirmação e o sequenciamento da atualização.

O BGP é o protocolo de roteamento da Internet global, bem como das redes privadas do Service Provider. O BGP expandiu seu propósito original de levar informações de acessibilidade à Internet e agora pode transportar rotas para Multicast, IPv6, VPNs e uma variedade de outros dados.

BGP (IETF)- O BGP é um protocolo de roteamento entre sistemas autônomos (ASs). Roteamento Baseado em Política (policy-based routing), um roteamento com base em um conjunto de regras não técnicas, definidas pelos Sistemas Autônomos.
Quando um roteador se conecta à rede pela primeira vez, os roteadores BGP trocam suas tabelas de rotas completas. De maneira similar, quando a tabela de rotas muda, roteadores enviam a parte da tabela que mudou. Roteadores BGP não enviam regularmente atualizações de roteamento planejadas e as atualizações de rotas informam somente a trajetória ótima para uma rede.

O BGP suporta dois tipos de trocas de informações de roteamento: trocas entre diferentes ASs e trocas dentro de um único AS. Quando usado entre ASs, o BGP é chamado BGP externo (EBGP) e as sessões BGP executam o roteamento inter-AS . Quando usado dentro de um AS, o BGP é chamado BGP interno (IBGP) e as sessões do BGP executam o roteamento intra-AS

Os 4 tipos de mensagens BGP são:

1. Abertura (open message) – abre uma sessão de comunicação entre BGP pares (peers) e é a primeira mensagem enviada de cada lado depois que uma conexão de protocolo de transporte é estabelecida; essa mensagem é confirmada usando uma mensagem de keep-alive enviada pelo roteador par e tem que ser confirmada antes das atualizações, notificações e outras mensagens de keep-alive.

2. Atualização (update message) – é usada para informar atualizações de rotas para outros sistemas BGP, permitindo que os roteadores possam construir uma visão consistente da topologia da rede, usando o TCP para garantir uma entrega confiável; essas mensagens podem retirar rotas inviáveis (unfeasible routes) da tabela de roteamento e simultaneamente informar uma nova rota.

3. Notificação (notification message) – é enviada quando uma condição de erro é detectada; elas são usadas para encerrar uma sessão ativa e informar a quaisquer roteadores conectados do porque do encerramento da sessão.

4. Keep-alive – notifica aos roteadores BGP pares que um dispositivo está ativo.

3 tipos de roteamento protocolos de roteamento e sua principal caracteristica.

Distance vecto - Não conhece toda a topologia da rede.Conhece somente os seus vizinhos e atraves deles começa a conhecer os prefixos da rede. Ex: EIGRP e RIPv2
Link state - Cada roteador conhece tem a topologia da rede. Os prefixos da rede são divulgados somente após alguma atualização. Ex: OSPF
Path vecto - Atributos utilizados para escolha do melhor caminho. Ex: BGP

EIGRP

Protocolo propretario da CISCO.

É conhecido como distance vector avançado pois combina caracteristicas de distance vecto e link state.

-Convergencia rapida;
-Updates parciais;
-Metricas sofisticadas;
-Suporta VLSM - Mascara de subnet de tamanho variavel;
-Multiplos protocolos de nível 3;

Confiavel no transporte, ele roda acima do protocolo ip.
Divulga em Multicast 224.0.0.10

#show ip eigrp neighbors
#show ip eigrp neighbors detail

#show ip eigrp interfaces
#show ip eigrp interfaces detail

#show ip protocols

#show ip router

D - EIGRP
O - OSPF
IA - OSPF Inter area
E1 - OSPF External
B - BGP
H - NHRP

AS (Autonomous systems) - Conjunto de roteadores, redes, links administrados por uma entidade. Rodando o mesmo protocolo de roteamento.
AS privado e AS publico.

Update porta 179 confiavel.

EBGP - Distancia Administrativa 20
IBGP - Distancia Administrativa 200

So envia update quando houver atualização. Incremental.
Utiliza KeepAlive para confirmar conectividade.

BGP estrutura

-BGP neighbor Table
.Lista dos vizinhos e seus estatus;
.Enviados keep-alive para manter essa vizinhança;

- BGP Table
.Lista de todas as redes aprendidas por todos vizinhos BGP;
.Indicação do caminho mais adequedo ataves dos atributos;

-Ip route table
.Pega na BGP table indicação do caminho mais adequedo

#show ip bgp summary
#show ip bgp neighbor
#show ip bgp (BGP Table)

Status do BGP

1.Idle - Tabela de rota checando o vizinho

2.Connect - Achou o vizinho handshake.

3. Open sent - Parametros estão sendo trocados.

4. Active - Não funcionamento. Vizinho com endereço errado. O ip do AS não existe. O vizinho não consegue fazer vizinhança comigo.

5. Open confirm - Negociação completa

6. Established - Estabeleceu sessão entre os vizinhos.

OSPF

O protocolo protocolo OSPF (Open Shortest Path First) foi desenvolvido pelo IETF (Internet Engineering Task Force) como substituto para o protocolo RIP e caracteriza-se por ser um protocolo intra-dominio ou interno (IGP – Interior Gateway Protocl), hierarquico, baseado no algoritmo de Estado de Enlace (Link-State), o qual foi especificamente projetado para operar com redes grandes.

Suporte hierárquico – Divisão lógica de um SA em áreas
• Uma ou mais redes em um domínio administrativo
• Cada área possui um BD de estado de enlace distinto
– Uma área não conhece a topologia da outra
– Mesmo protocolo de roteamento
– Área de backbone ou Área 0
• Área obrigatória • Responsável pelo roteamento entre outras áreas do AS
– Link virtual • Situações em que não é possível estabelecer conexão direta com a área 0

Classes de roteadores
– Internos (única área)
– Borda de área – De backbone
– De fronteira do SA
Centralização
– Vizinhos
• Estão conectados fisicamente
• Descoberta por meio da mensagem HELLO
– Adjacentes •
Trocam informações de roteamento entre si
– Designados
• Adjacente a todos os roteadores
• Calcula e distribui todas as rotas
• Necessidade de roteador de backup

IPSEC

Trabalha na camada 3.
So trafega tráfego Unicast.Complemento com GRE.

Algoritimos IPSEC
Ipsec protocol - ESP | ESP+AH | AH
Confidencialidade - DES | 3DES | AES
Data integrity - md-5 | Sha-1 e sha-2
Origin Authentication - PSK | RSA
Key managentement - DH | IKEv2

Simetrica - A mesma chave que cifra é a mesma que decifra.
Assimetrica - São usadas duas chaves. Uma chave do proprietario e a outra publica.
Certificados digitais.

Ike - Responsável pelo acordo chave usando assimétrica criptografia

ESP - Fornece criptografia de dados, integridade de dados e peer autenticação; Protocolo IP 50

O ISAKMP é o protocolo que negocia a política e fornece uma estrutura comum gerando as chaves de que os IPsec peer compartilham. O ISAKMP usa a porta 500 UDP para a negociação.

Modo de transporte
O cabeçalho ESP ou AH é inserido atrás do cabeçalho IP; a
O cabeçalho IP pode ser autenticado, mas não criptografado

Modo de túnel
Um novo cabeçalho IP é criado no lugar do original; esta
permite a criptografia de todo o pacote original

Serviços e segurança oferecidos pelo IPSEC.

-Confidencialidade;
Capacidade de prover segurança a uma informação de um ponto a outro. Criptografia.

-Integridade;
Garantir que a informação n foi adulterada no caminho.

-Autenticação
Certeza que garanta que o host que vc esteja fechando vpn seja ele mesmo.

-Anti-replay protection
Substituição do frame. Atacante adulterar pacote.

IPSEC - Somente Unicast.
-IKEv2 - Protocolo que estabelece negociação.
-ESP - Criptografia e hash dentro do pacote protegido.

firewall UTM

Firewall é uma solução de segurança unificada que permite a gestão de forma centralizada de diversas funcionalidades de segurança da informação.

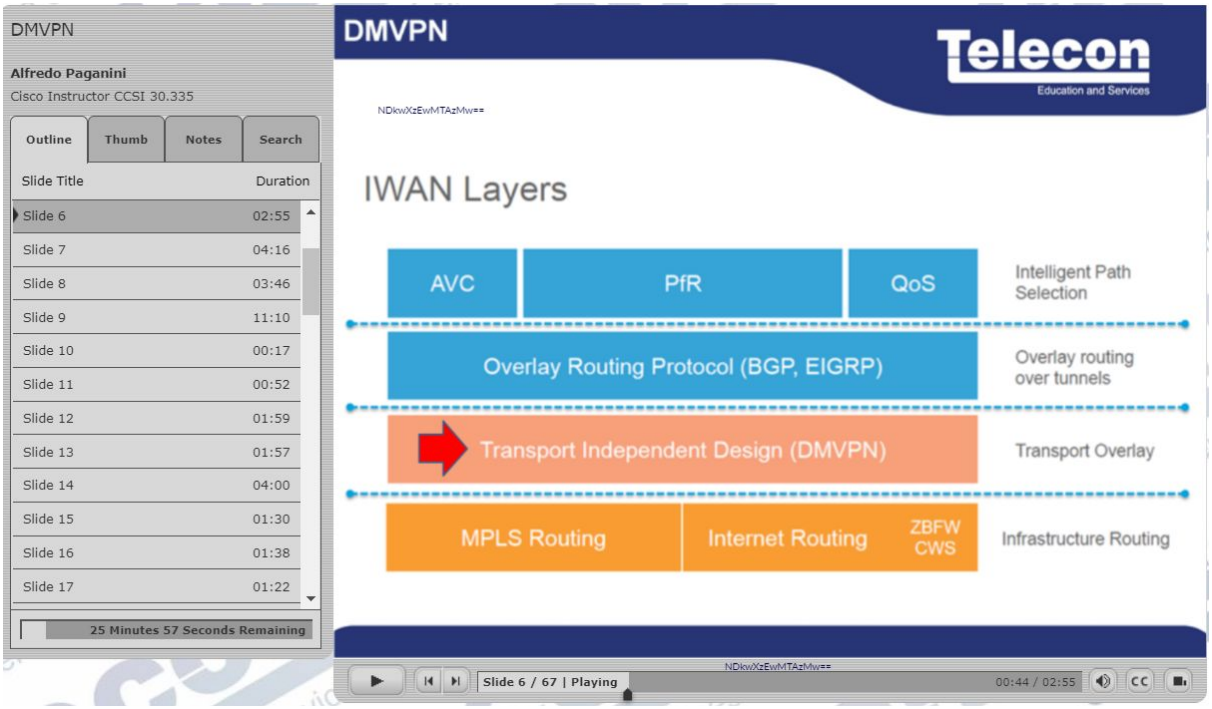
O principal ponto do firewall UTM é poder agregar muitas funcionalidades, com facilidade de gerenciamento e baixo custo, desta forma permitindo empresas que até então não poderiam ter um nível de segurança aceitável, a adquirir um único equipamento e obter resultados dignos de grandes empresas. Não à toa, grandes empresas têm adotado Firewall UTM como parte de sua estratégia de segurança.

As funcionalidades de um firewall UTM, incluem, mas não se limitam em:

- **NG Firewall;**
- **Servidor VPN;**
- **Antivírus de rede;**
- **IPS – Intrusion Prevention System;**
- **Filtro de conteúdo (proxy);**
- **Balanceamento de carga ou ADC application delivery control;**
- **Controle de acessos;**
- **Gestão de identidades;**
- **Web application firewall;**
- **Proteção de e-mail e Antispam;**
- **Proteção contra ameaças desconhecidas;**
- **Relatórios diversos;**

- **Sistema de gerencia unificado;**
- **Controle de conteúdo;**
- **WLAN Controller (Gerenciador de Access Points);**
- **SSL Inspection ou Visibilidade de trafego SSL;**
- **Cloud Sandbox;**
- **Roteamento;**
- **Controle de trafego, QoS e Shapping;**
- **Anti-DDoS;**
- **Sincronizaçao de segurança com Endpoint Protection;**

IP Addresses	Bits	Prefix	Subnet Mask
1	0	/32	255.255.255.255
2	1	/31	255.255.255.254
4	2	/30	255.255.255.252
8	3	/29	255.255.255.248
16	4	/28	255.255.255.240
32	5	/27	255.255.255.224
64	6	/26	255.255.255.192
128	7	/25	255.255.255.128
256	8	/24	255.255.255.0
512	9	/23	255.255.254.0
1 K	10	/22	255.255.252.0
2 K	11	/21	255.255.248.0
4 K	12	/20	255.255.240.0
8 K	13	/19	255.255.224.0
16 K	14	/18	255.255.192.0
32 K	15	/17	255.255.128.0


DMVPN
Alfredo Paganini
Cisco Instructor CCSI 30.335
Outline
Thumb
Notes
Search
Slide Title
Duration
Slide 6 02:55
Slide 7 04:16
Slide 8 03:46
Slide 9 11:10
Slide 10 00:17
Slide 11 00:52
Slide 12 01:59
Slide 13 01:57
Slide 14 04:00
Slide 15 01:30
Slide 16 01:38
Slide 17 01:22
25 Minutes 57 Seconds Remaining
DMVPN
Telecon
Education and Services
NDkwXzEwMTAzMw==
IWAN Layers
AVC
PfR
QoS
Intelligent Path Selection
Overlay Routing Protocol (BGP, EIGRP)
Overlay routing over tunnels
Transport Independent Design (DMVPN)
Transport Overlay
MPLS Routing
Internet Routing
ZBFW CWS
Infrastructure Routing
NDkwXzEwMTAzMw==
Slide 6 / 67 | Playing
00:44 / 02:55
CC