Notas SRC

Slide 2:

Vetores de ataque:
- Social engineering
- Vulnerabilidades

Fases:
- Infiltração através de social engineering e pode conter instalação de software illicit.
- Propagação através de credenciais roubadas e vulnerability exploitation.
- Internal aggregation and exfiltrate information, for example in metadata.

Slide 4:

Network security systems:
- Firewall
- IPS: analyzes packets, but can also stop the packet from being delivered
- IDS: analyze network traffic for signatures that match known cyberattacks
- Security appliances

Firewall: It is a system or group of systems that enforces a control policy between two or more networks.
It can perform NAT, Authorization, Redirecting, Content analysis, VPN's and DoS and DDoS defense.

The network must be protected at multiple levels and locations, not only on the perimeter of the internet.

Stateful vs Stateless Firewall:
- Stateless: Applies rules to single frames/packets about packet headers (ACL). Ideal for DDoS 1ºst line of defense.
- Stateful: Applies rules to all traffic flows. It takes into account the connection state and bidirectional rules can be applied. Connections are maintained in a state table. In load balancing scenarios must be synchronized.

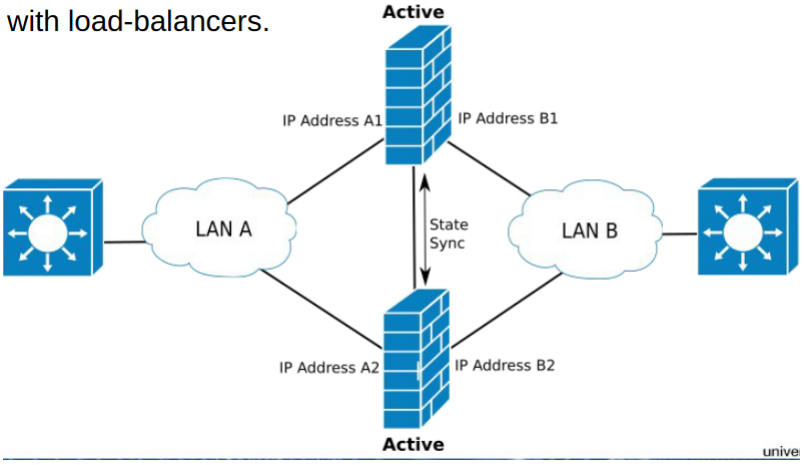
Firewall Zones: Collection of ip, networks or ports that divide a network with different security levels. The firewall rules will use these zones as either a source or destination.

Firewall virtual instances: A virtual firewall instance can handle different zones/groups, all from the same machine.

High availability scenario:

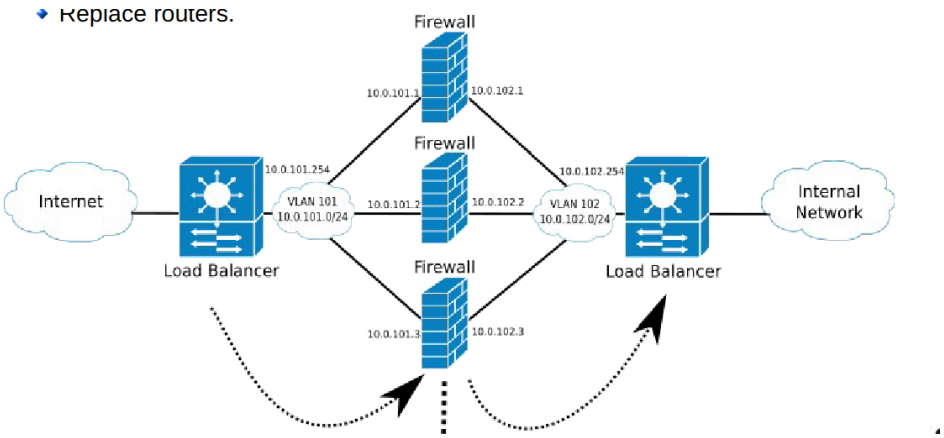
- Active-backup: Firewalls share state normally via dedicated connection (state sync), shared Virtual IP (VRRP) and backup is only used when main fails.
- Active-active: Firewalls share state too (state sync), but share load and work with load balancers. have dedicated ip's.

with load-balancers.



Load balancers with firewalls advantages:

- Decrease processing and memory requirements for each firewall
- Allow scalability
- Less vulnerable to DDoS
- No need to State share Firewalls.



Load Balancing algorithms:

- IP Hash: The ip address is used to determine which firewall receives the flow. No state table, hash function determines output
- Round Robin: Requests sequentially, firewalls have to share state

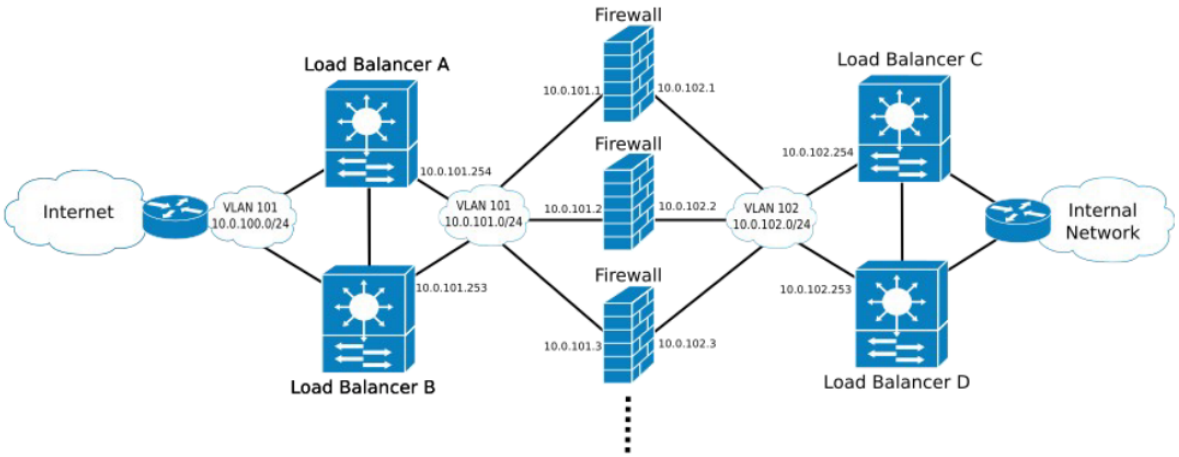
- Least Connections: Request to the firewall with least connections.
- Smart: external info.

Firewalls provide routing with ips.

Stealth Firewalls: Operate at layer 2, with no ip and forward packets from one vlan to another, or one interface to another (802 1q is layer 2)

Load balancers can have separate virtual instances for different zones with different firewalls for each.

Redundant load balancers:
- Balancers share routing history.



Stealth doesn't have ip's.

Best Practiced and recommendations:
- Standardize security policies
- Block traffic by default
- Maintain documentation of firewall rules
- Maintenance of rules

Ip spoofing:
- Forged source ip

Stop ip spoofing at layer 3:
- Deny external traffic with source ip of the protected network range. (local)
- Ip source equals private address. (192.168.1.0/16, 10.0.0.0/8, 172.16.0.0/12)
- Multicast destinations. (224.0.0.0/24)

Stop ip spoofing at layer 2:
- Check the DHCP server to verify the ip address of the untrusted layer 2 port where traffic is generated. If it's a different block. Enabled on untrusted layer 2 ports with DHCP. LAYER 2 FIREWALL.

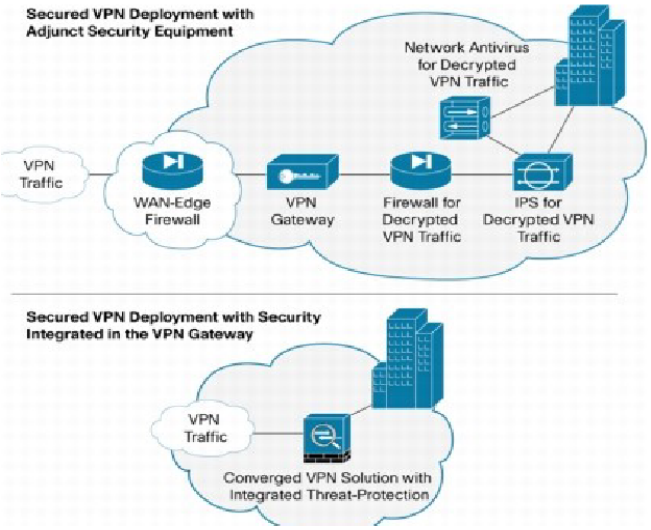
Half Open Tcp connections attack:

- Firewall keeps the state of the TCP session in memory
- Multiple half-open tcp sessions can overrun a firewall.
- To solve this, lower timeout values must be set specially during attack
- Externally clean these connections.

DDOS mitigation at source: Committed access rate (car)

- The CAR is configured on a port and limits certain input / output traffic to a specific rate.
- Avoids that a single source may generate/transmit traffic above a threshold.
- Establish a rule where the rate is higher when the tcp session is established vs when it is not on the output port for the firewall to the server that is under attack(2 access lists).
- https://www.ciscopress.com/articles/article.asp?p=345618&seqNum=5

Firewalls and VPN have to work together, since the packet will be protected until it arrives at the vpn gateway, it needs to have a firewall after to check for traffic. Most firewalls integrate both Security and VPN gateway services.



Slide 5:

Public Key encryption:

- To send an encrypted message from A to B
  - Host A encrypts data with Host B public key (PUB)
  - Host B decrypts data with Host B private key (PRB)

Normally negotiate a symmetric key, with the public key encryption.

- To send an authenticated message from A to B
  - Host A creates a signature by encrypting data with Host A private key (PRA)
  - Host A sends data and signature to host B
  - Host B verifies date by decrypting signature with Host A public key (PUA) and compares with received message

Public key Infrastructure:

- Each PKI participant holds a digital certificate that has been issued by a Certificate Authority (CA)

Simple Certificate Enrollment Protocol:

- 1: Generate key pair
- 2: send certificate request to CA with public key
- 3: Manual approval by the CA
- 4: After approval the CA signs the certificate with it's private key and sends to the host
- 5: Host stores the signed certificate.

CRL: list where certificates are revoked.

To verify 3 steps:

- Is the certificate valid?
- Is the root CA known and trustable?
- Is the certificate on the revocation list?

Virtual Tunnel Interface: Virtual network interface for the tunnel

The main advantage of using loopback interfaces as tunnel end-points, is the creation of a tunnel not bound to any individual network card/link that may fail.

Overlay network: virtual network defined over another network, when a privacy protocol is presented on the overlay network, it's a VPN.

Multi point tunnel: Tunnels with more than one destination / source. The overlay network has multiple ip's and the tunnel end-points also have multiple ip's that are routed by different next-hop.
Next Hop Resolution Protocol (NHRP): Associates tunnel destination address with the respective underlying network.
As you set the for example, the static route to the next hop of the overlay network and the destination on the tunnel, when multiple destinations exist, the tunnel has to know to which destination it has to send, according to the next hop overlay network.
Hub-Spoke: Each remote site is connected to the hub and he relays data.
Spoke-Spoke: Each node can dynamically initiate tunnels between each other.

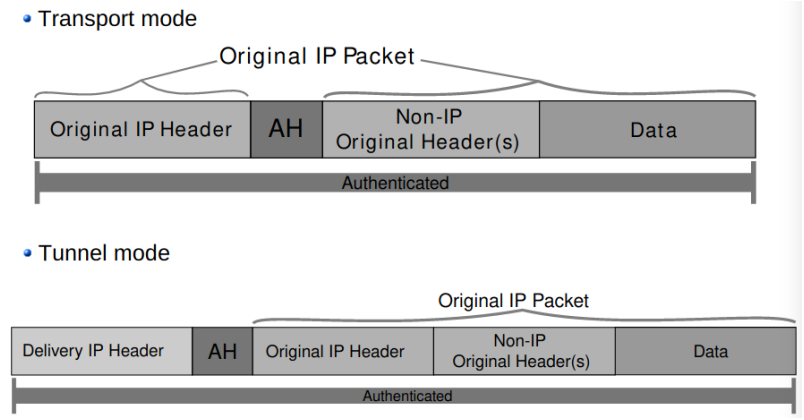
IPSec:

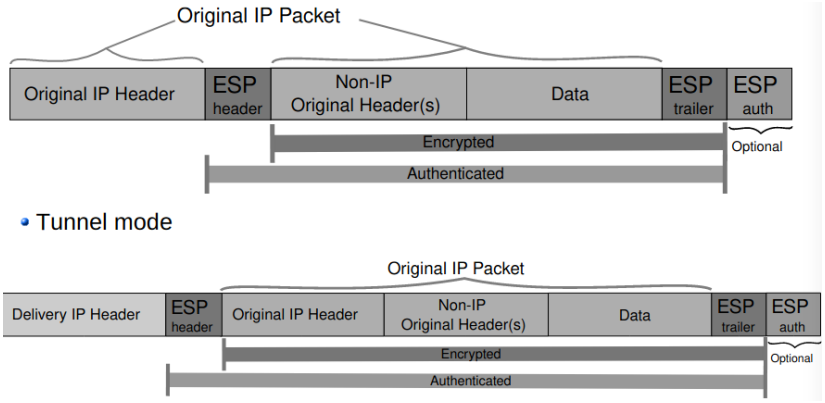
AH -> authentication header guarantees data integrity.

ESP -> Provides encryption and data integrity.

Modes:
-> Tunnel: Ipsec gateways provide Ipsec services to other hosts.
-> Transport: IPSec host to host, has to be implemented on end-hosts.

(...)





VPN: encrypted connection between private networks over a public network.

Remote Access VPN: Normal user vpn.
- PPTP
- OpenVPN

Site-to-Site:
- IPsec
- IPsec + GRE

The ISAKMP works as following:
- The security association proposal is sent and the other side responds if he agrees on parameters
- The diffie hellman exchange happens
- The next packets are encrypted with the shared diffie key.

The ISAKMP can use either a pre-shared key or Public key encryption.

Slide 6:

Most common remote access servers:

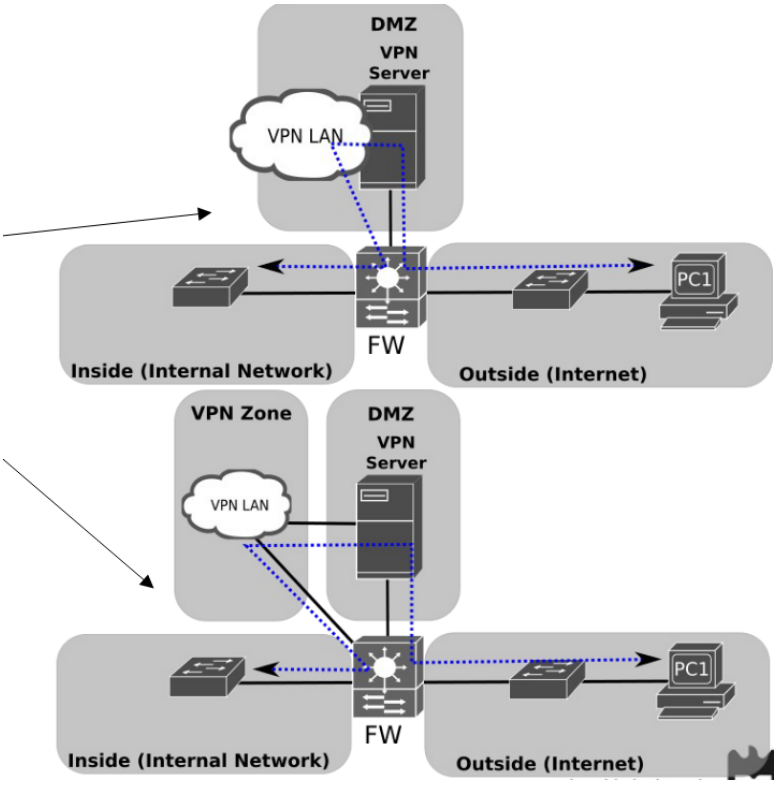
- L2TP IPsec
- OpenVPN

Authentication types:

- Pre-shared
- RSA with embedded CA
- RSA with external CA

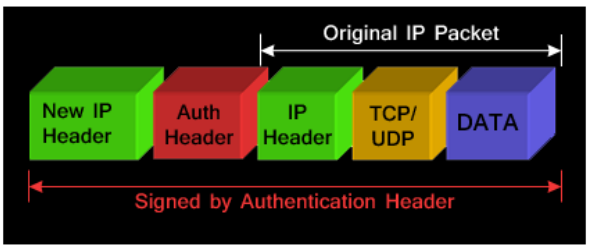
shu

Na situação em que existe um servidor VPN na DMZ, a ponta do túnel vai ser o servidor VPN, neste caso encontra-se na zona do DMZ.
Para não quebrar o conceito de zona, faz sentido que esses ip's estejam a ser protegidos pela firewall noutra zona, porque já se podem aplicar outras políticas que não se aplicam a DMZ.
O ip do novo user vai para o default gateway de VPN server!

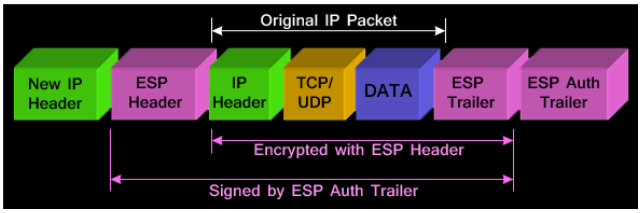


IPsec incompatível com NAT/PAT:

- No modo AH, porque neste modo todo o pacote (incluindo o das pontas dos túneis) é verificado pelo AH.



Isto significa que se existir um processo de tradução de NAT, o new ip header (pontas do túnel) faz com o AH fique incompatível.



- No caso do ESP não há stress porque não são autenticados com o AH nas pontas do túnel.

- Existe um modo especial que permite isto, enviando um NAT-OA (Nat original address) payloads no ISAKMP

Regras para as flows do utilizador:
- Utilizadores são associados uma gama de ip
- Controlo de fluxos baseado no ip de origem ou zona VPN.

Slide 7:

Intrusion detection system (IDS):
- Monitors and identifies unauthorized system access or manipulation.
- Analyzes information from multiple sources (Network traffic, servers, services etc).
- Identifies Intrusions and misuse.
- Does not block intrusion
- Signals alarms for humans or firewalls automatic threat responses.

Intrusion protection system (IPS):
- Can block traffic
- Can kill processes, quarantine files, block device access etc.

Host-Based: Deployed on servers or devices.
Network-Based: Deployed at the network level, deployed at multiple network points.

Intrusions are detected based on 2 approaches:
- Signature data: Monitor data compared with predetermined attack patterns (signatures), signatures may contain individual packet headers, binary data patterns, Sequence of packets with specific characteristics on the same flow, or a set of data flows.
- Anomaly based: Establishes a behavior profile and detects deviations from that profile, may use AI models to determine a behavior profile.

Both IDS and IPS are network taps, but the IPS communicates with the firewall to block.

Slide 8:

Data sources:

SNMP - Local information about current node state.
Flow exporting - Characterize users/services in terms of amount of traffic and traffic destinations
Packet Captures
Access server Logs

SNMP:
- Used for acquiring the status and usage of nodes, links and services over time

- Requires periodic pulling

Netflow:
- Ip flow information from data networks.
- Used to characterize user/services in terms of amount of traffic.
- Traffic matrices: from point a to all possible points

Network Monitoring:
- Specific and detailed data analysis
- Infer small and medium time scales
- Can be a network tap, switch mirror port or in line
- Can be filtered
- Packet information

Remote CLI Access:
- Ssh to retrieve device state

Rsyslg:
- Accept input from multiple services and transform them and output to network.
- Timing controller by device

Direct Access to log files:
- sftp
- Timing controlled by central point

Log management systems:
- Aggregates log files.
- Organizes them in a centralized solution
- Detect IOCs
- Conduct data forensics

Security Information and Event Management (SIEM):
- SEM: Similar ao LMS, agrega os logs todos dos sistemas, mais virado para IT
- SIM: Identificar dados dos eventos dos logs, alertas automáticos em condições que a rede está comprometida
- SEC: Correlacionar eventos e ligações que detectem um problema.

LMS vs SIEM:
- LMS mais virado para reter os logs de maneira eficiente, e pesquisa fácil
- SIEM detectar ataques, correlacionar eventos, e dashboard em real time.