



SEC+

Lesson 5:

Maintain Enterprise Campus Network Architecture

Objectives

- Compare and contrast security implications of different on-premises network architecture models
- Apply security principles to secure on-premises network architecture
- Select effective controls to secure on-premises network architecture
- Ensure secure communications for remote access and tunneling

Lesson 5

Topic 5A

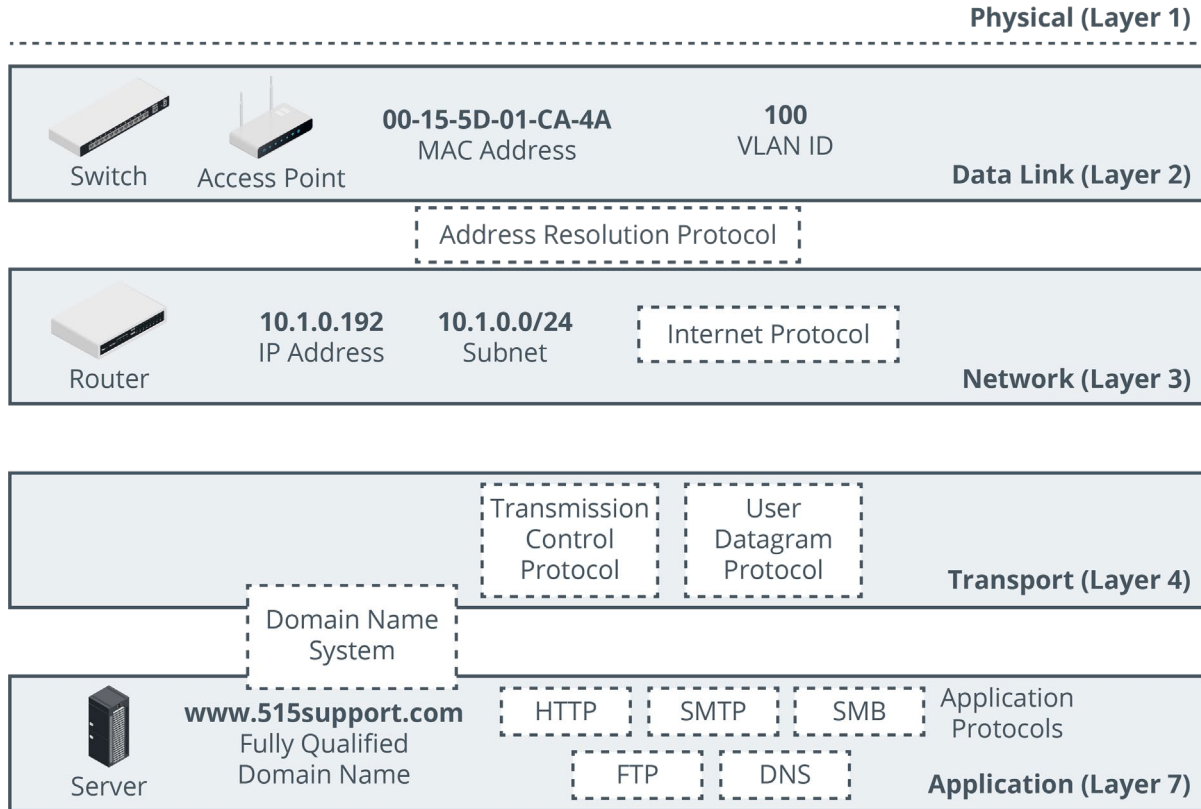
Enterprise Network Architecture



Architecture and Infrastructure Concepts

- Selection and placement
 - Infrastructure (media, appliances, addressing/forwarding for connectivity)
 - Applications/services
 - Data
- Workflows
 - Access
 - Email mailbox server
 - Mail transfer server

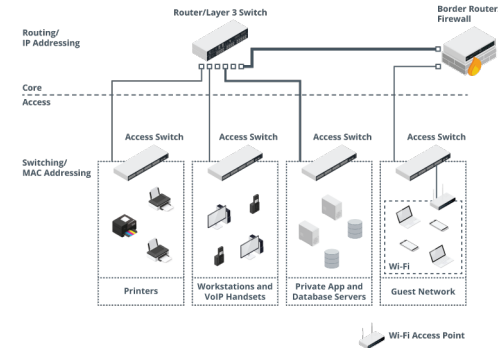
Network Infrastructure



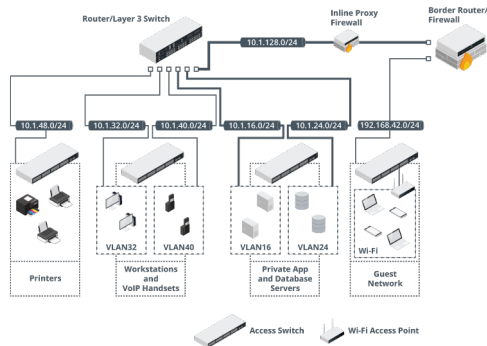
Images © 123rf.com.

Switching Infrastructure Considerations

- Topology of nodes and links
 - Physical versus logical
- On-premises networks
 - Office/campus
 - Structured cabling
- Hierarchical design
 - Limit size of broadcast domains
 - Enforce segmentation



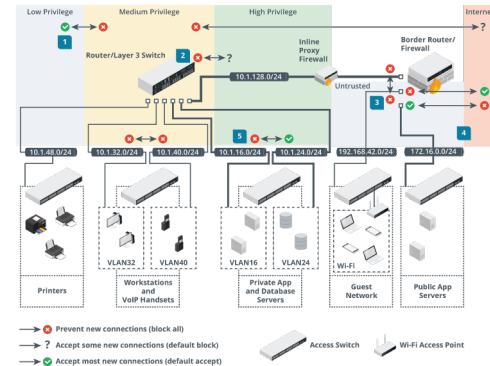
Routing Infrastructure Considerations



- Layer 3 logical segmentation
 - Networks and subnetworks (subnets)
- Internet Protocol (IP)
 - IPv4 and IPv6
 - Network prefix/subnet mask
- Virtual LAN (VLAN)
 - Map layer 2 switch port topology to layer 3 IP subnet topology
 - Makes logical topology independent of port location on physical switches

Security Zones

- Segment containing hosts with same access control/security requirements
 - Public versus private
 - Database and file servers
 - Compartmentalize different types of data assets
 - Client devices
 - Public-facing app servers
 - Network infrastructure servers



Attack Surface

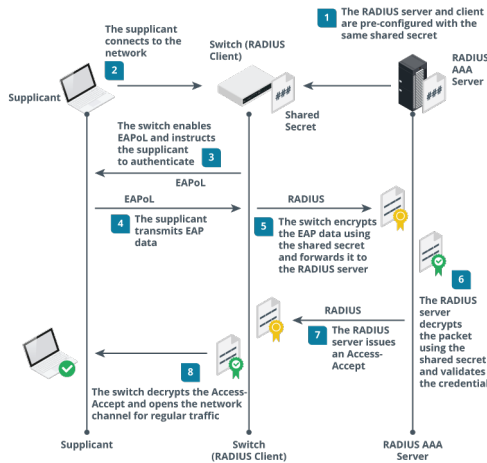
- Points at which threat actor can gain access
 - Layer 1/2 versus layer 3 versus layer 4/7
- Defense in depth and layered security controls
- What problems arise from weaknesses in the network design/architecture?
 - Single points of failure
 - Complex dependencies
 - Availability over confidentiality and integrity
 - Lack of documentation and change control
 - Overdependence on perimeter security

Port Security

- Physical port security and administratively disabled ports

- MAC filtering and limiting

- 802.1X, EAP, and RADIUS



- Supplicant (user's computer)

- Authenticator/RADIUS client (switch)

- Authentication/RADIUS server

- IEEE 802.1X allows switches to implement EAP over LAN (EAPoL)

- Extensible Authentication Protocol (EAP) provides framework for authentication methods/factors

- Remote Authentication Dial-in User Service (RADIUS) allows use of a directory of user accounts and credentials

Physical Isolation

- Single host or group of hosts not connected to any other network
 - Air gapped
- Difficult to manage
 - Updates via media devices

Architecture Considerations (1)

- Cost
 - Upfront capital cost and loss of value through depreciation
 - Ongoing maintenance and support
- Compute and responsiveness
 - Reduce workload processing time
- Scalability and ease of deployment
 - Minimize costs associated with increasing (or decreasing) workloads

Architecture Considerations (2)

- Availability
 - Minimize downtime
- Resilience and ease of recovery
 - Reduce time taken to recover from failures
- Power
 - Costs of high compute resources and reliability of infrastructure
- Patch availability
 - Mitigate vulnerabilities
 - Inability patch due to third-party management or lack of vendor support
- Risk transference
 - Contracting infrastructure to third-parties

Enterprise Network Architecture

- Architecture and infrastructure concepts
 - Media, applications/services, data supporting workflows
- Network infrastructure
 - OSI layer model
- Switching and routing infrastructure considerations
- Security zones and attack surface
- Port security and physical isolation
 - MAC filtering, 802.1X/EAP/RADIUS
- Architecture considerations
 - Cost, compute/responsiveness, scalability/ease of deployment, availability, resilience/ease of recovery, power, patch availability, risk transference

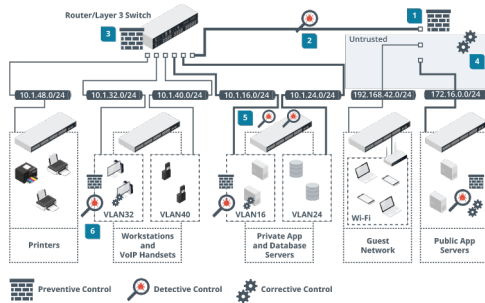
Lesson 5

Topic 5B

Network Security Appliances



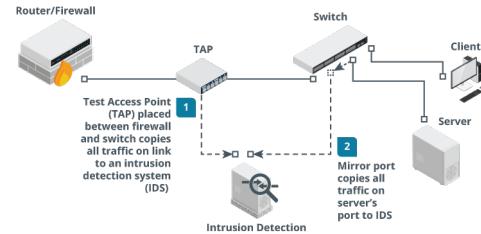
Device Placement



- Selection of effective controls
 - Enforce segmentation, apply access controls, monitor traffic
- Defense in depth
 - Zone border (mostly preventive)
 - Within zone (mostly detective)
 - Endpoint controls (preventive, detective, and corrective)

Device Attributes

- Active versus passive
 - Passive controls don't require hosts to be configured to use them (and might not be detectable by hosts)
 - Active controls require host configuration or software agents
- Inline versus tap/monitor
 - Inline is installed as part of cable path ("bump-in-the-wire")
 - Switched port analyzer (SPAN) or mirror port
 - Test access point (TAP)
- Fail-open
 - Preserves access on fail to prioritize availability
- Fail-close
 - Prevents access on fail to priorities confidentiality/integrity



Firewalls

- Enforce a network access control list (ACL)
- Packet filtering inspects headers only
 - Source and destination IP address
 - Protocol ID/type (TCP, UDP, ICMP, routing protocols, and so on)
 - Source and destination port numbers (TCP or UDP application type)
 - Drop/deny/reject or accept/permit a packet (and/or log)
 - Inbound, outbound, or both
- Placement and attributes
 - Routed, bridged, or inline placement
 - Firewall appliance versus router firewall

The screenshot displays the OPNsense web interface for a device named 'Lobby'. The interface includes a sidebar menu with options like Dashboard, License, Password, Logout, Reporting, System, Interfaces, Firewall, VPN, Services, Power, and Help. The main content area is titled 'Lobby: Dashboard' and contains several widgets:

- System Information:** A table showing system details such as Name (gw.ad.structureality.com), Versions (OPNsense 23.1.9-amd64, FreeBSD 13.1-RELEASE-p7, OpenSSL 1.1.1t 7 Feb 2023), Updates (Click to check for updates), CPU type (Intel(R) Xeon(R) CPU E5-2690 v4 @ 2.60GHz), CPU usage (100%), Load average (0.45, 0.38, 0.19), Uptime (00:07:48), Current date/time (Tue Jun 6 11:03:32 CDT 2023), Last config change (Tue Jun 6 10:58:33 CDT 2023), and CPU usage (0%).
- Gateways:** A table listing gateways with columns for Name, RTT, RTTd, Loss, and Status. Two gateways are shown: WAN_GW4_515web (203.0.113.6) and LAN_GW4 (10.1.128.254), both with Online status.
- Interfaces:** A section for network interfaces.
- Traffic Graph:** A line graph showing network traffic in (bps) over time, with a peak around 3.00 K.

At the bottom of the dashboard, there is a footer: OPNsense (c) 2014-2023 Deciso B.V.

Layer 4 and Layer 7 Firewalls

- Stateful inspection validates connections
 - State table stores connection information
- Transport layer (layer 4)
 - TCP handshake
 - New versus established and related connections
- Application layer (layer 7)
 - Validate protocol and match threat signatures
 - Application layer gateway, stateful multilayer inspection, or deep packet inspection
 - Application-specific filtering

Firewall: Diagnostics: States Select rule

States **Actions**

Search 7

<input type="checkbox"/>	Int	Dir	Proto	Source	Nat	Desti...	State	Rule	Commands
<input type="checkbox"/>	all	←	icmp	203.0.11...		203.0.11...	0:0	let out a...	
<input type="checkbox"/>	all	→	tcp	10.1.24...		10.1.128...	ESTABLI...	anti-loc...	
<input type="checkbox"/>	all	→	tcp	165.88.7...		203.0.11...	SYN_SE...	Mail gat...	
<input type="checkbox"/>	all	→	tcp	1.111.22...		203.0.11...	SYN_SE...	Mail gat...	
<input type="checkbox"/>	all	→	tcp	213.86.1...		203.0.11...	SYN_SE...	Mail gat...	
<input type="checkbox"/>	all	→	tcp	53.92.25...		203.0.11...	SYN_SE...	Mail gat...	
<input type="checkbox"/>	all	→	tcp	38.20.16...		203.0.11...	SYN_SE...	Mail gat...	

Showing 1 to 7 of 74 entries

OPNsense (c) 2014-2023 Deciso B.V.

Screenshot used with permission from Rubicon Communications, LLC

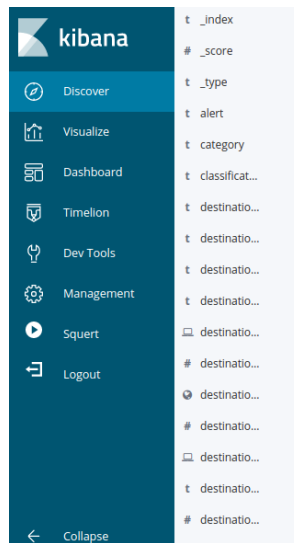
Proxy Servers

- Forward proxy server
 - Proxy opens connections with external servers on behalf of internal clients
 - Application-specific filters
 - Non-transparent and transparent proxies
 - User authentication
- Reverse proxy server
 - Proxy opens connections with internal servers on behalf of external clients

The screenshot shows the OPNsense Administration interface for the 'Web Proxy' service. The left sidebar contains a navigation menu with items like 'DHCPv6', 'Dnsmasq DNS', 'Intrusion Detection', 'Monit', 'Network Time', 'Net-SNMP', 'Ntopng', 'OpenDNS', 'Postfix', 'Redis', 'Rspamd', 'Unbound DNS', 'Web Proxy', 'Administration', 'Cache Log', 'Access Log', and 'Store Log'. The main content area is titled 'Services: Web Proxy: Administration' and features a search bar at the top right. Below the title are several tabs: 'General Proxy Settings', 'Forward Proxy', 'Proxy Auto-Config', and 'Remote Access Control Lists'. The 'Forward Proxy' tab is active, showing a 'Support' link and an 'advanced mode' toggle. The main configuration area includes several sections: 'Allowed Subnets' with a text input field and 'Clear All'/'Copy' buttons; 'Unrestricted IP addresses' with a text input field and 'Clear All'/'Copy' buttons; 'Banned host IP addresses' with a text input field containing '203.0.113.66' and 'Clear All'/'Copy' buttons; 'Whitelist' with a text input field containing 'Regular expressions are allowed.' and 'Clear All'/'Copy' buttons; and 'Blacklist' with a text input field containing 'example.com' and 'Clear All'/'Copy' buttons. An 'Apply' button is located at the bottom of the configuration area. The footer of the interface reads 'OPNsense (c) 2014-2023 Deciso B.V.'.

Intrusion Detection Systems

- Sensor captures traffic
 - Placement
 - Inline versus mirror/tap/monitor
- Intrusion Detection System (IDS)
 - Detection engine performs real-time analysis of indicators
 - Passive logging/alerting
- Intrusion Prevention System (IPS)
 - Active response (block, reset, redirect)
 - Inline response versus integration with other security tools



Time - source

March 16th 2020, 13:57:40.947 destination_ips: 195.2.253.92 message: [1:2003380:12] ET USER_AGENTS Suspicious User-Agent - Possible Trojan Downloader (ver18/ver19 etc) [Classification: A Network Trojan was detected] [Priority: 1]: <siem-eth1-1> {TCP} 192.168.3.35:1037

Table JSON View surrounding documents View single document

@timestamp	March 16th 2020, 13:57:40.947
@version	1
_id	BQyi43ABPEdm6QZiyTo1
_index	siem:logstash-ids-2020.03.16
_score	-
_type	doc
alert	ET USER_AGENTS Suspicious User-Agent - Possible Trojan Downloader (ver18/ver19 etc)
category	user_agents
classification	A Network Trojan was detected
destination_geo.continent_code	EU

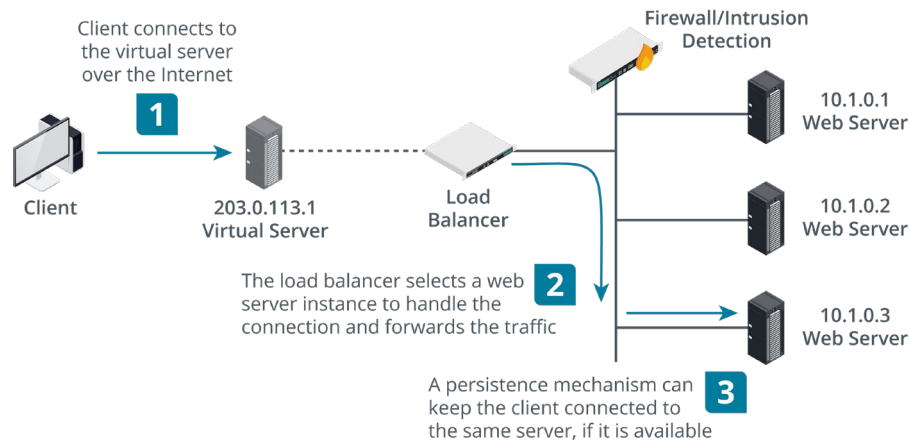
Screenshot Security Onion securityonion.net

Next-generation Firewalls and Unified Threat Management

- Next-generation firewall
 - Application-aware filtering, user account-based filtering, IPS, cloud inspection, ...
- Unified threat management (UTM)
 - Combining security controls into single agent and management platforms
 - Firewall, anti-malware, network intrusion prevention, spam filtering, content filtering, data loss prevention, VPN, cloud access gateway, ...

Load Balancers

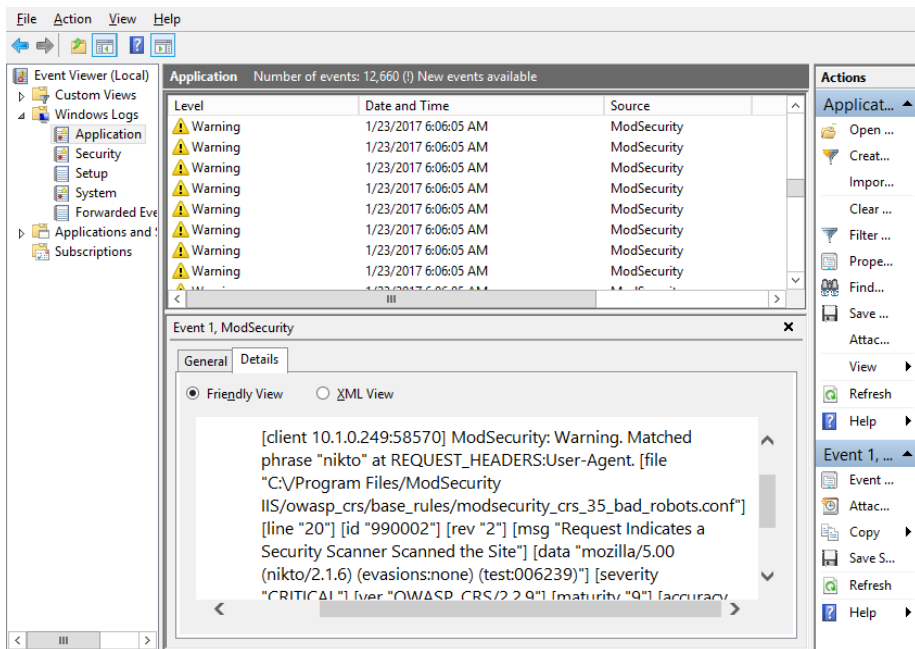
- Distributes requests across farm or pool of servers (nodes)
 - Layer 4 load balancer
 - Layer 7 load balancer (content switch)
- Scheduling
 - Round robin
 - Fewest existing connections / best response time
 - Weighting
 - Heartbeat and health checks
- Source IP affinity
- Session persistence



Images © 123rf.com.

Web Application Firewalls

- Able to inspect code in HTTP packets
- Matches suspicious code to vulnerability database
- Can be implemented as software on host or as appliance



Network Security Appliances

- Device placement
 - Defense in depth plus use of preventive, detective, and corrective controls
- Device attributes
 - Active versus passive, inline versus TAP/monitor, fail-open versus fail-closed
- Firewalls (layer 4/7)
- Proxy servers
- Intrusion detection systems
- Next-generation firewalls and unified threat management
- Load balancers
- Web application firewalls

Lesson 5

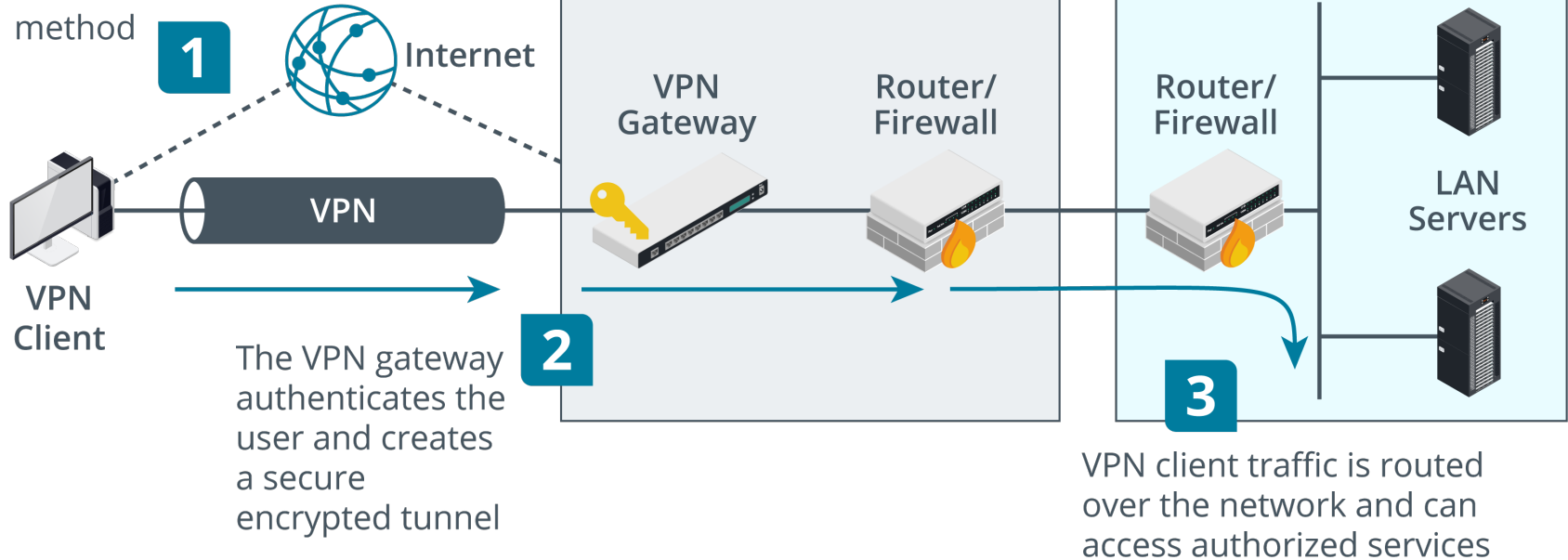
Topic 5C

Virtual Private Networks



Remote Access Architecture (1)

The VPN client host connects to a VPN gateway using any type of Internet subscriber access method

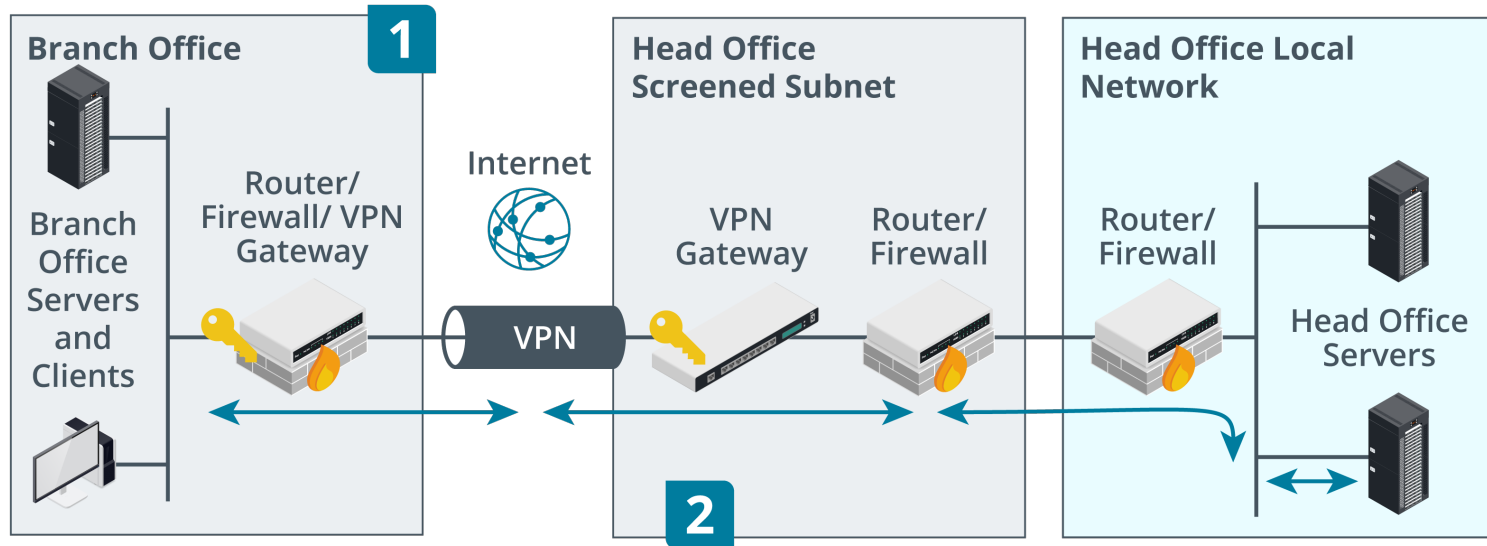


The VPN gateway authenticates the user and creates a secure encrypted tunnel

VPN client traffic is routed over the network and can access authorized services

Remote Access Architecture (2)

The VPN gateway at a branch office establishes a VPN connection with the head office site

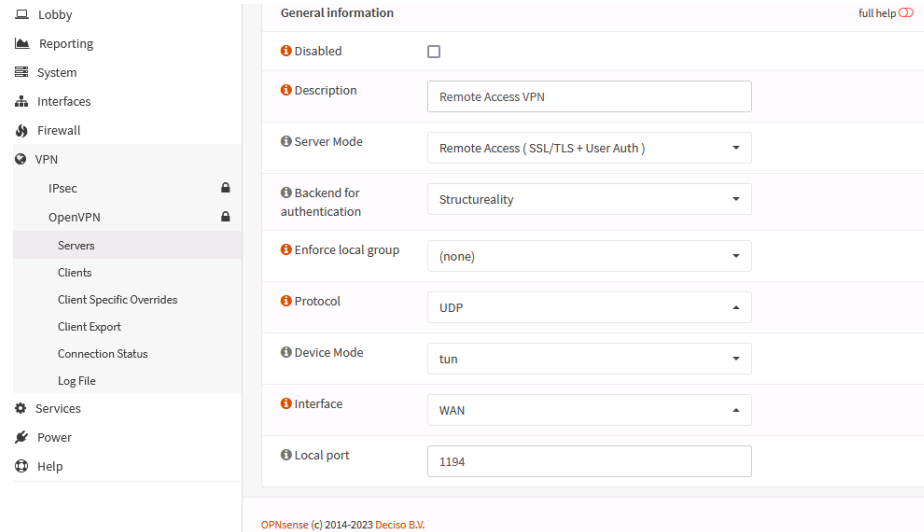


Traffic for a host at a remote site is automatically routed and tunneled over the VPN link

Images © 123RF.com.

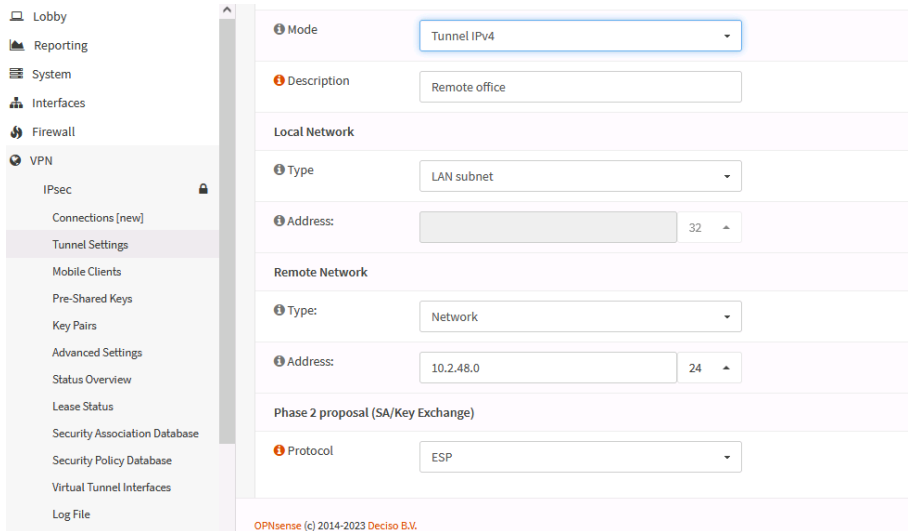
Transport Layer Security Tunneling

- Use TLS to negotiate a secure connection
 - Machines authenticated by PKI certificates
 - Mutual authentication allows VPN gateway to authenticate client certificates
 - User account authentication via RADIUS
- Tunnel network traffic over TLS
- Can use TCP or UDP



Screenshot used with permission from Rubicon Communications, LLC.

Internet Protocol Security Tunneling



- Provides confidentiality and/or integrity
 - Authentication Header (AH)
 - Signs packet but does not encrypt payload
 - Provides authentication/integrity only
 - Encapsulation Security Payload (ESP)
 - Provides confidentiality and/or authentication/integrity
- Modes
 - Transport mode for host-to-host connections on a private network
 - Tunnel mode between gateways across an unsecure network

Internet Key Exchange

- Establishes Security Association (SA) between peers
- Phase I provides authentication
 - PKI/certificates
 - Pre-shared key
- Phase II establishes cipher suites and key sizes and use of AH or ESP
- IKE v1 supports host-to-host and site-to-site tunneling
- IKE v2 adds better support for client-to-site remote access VPN

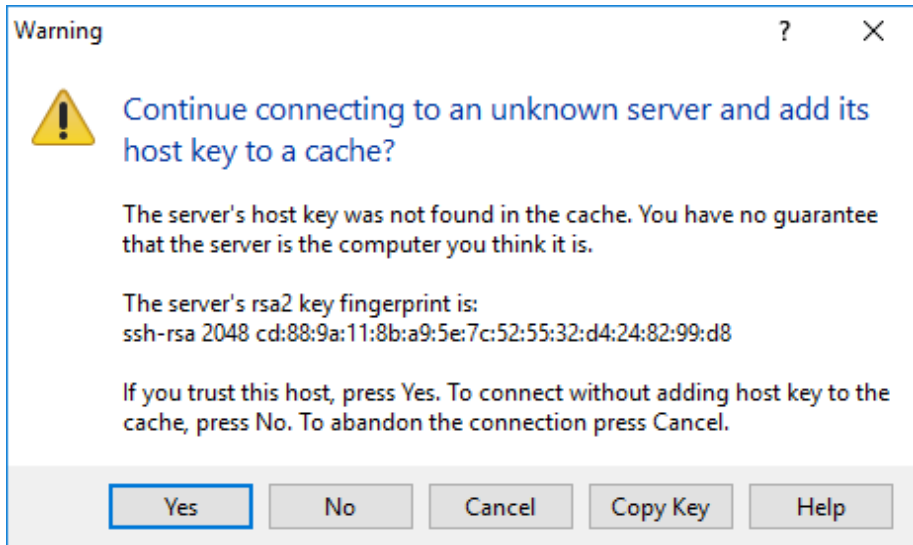
Phase 1 proposal (Authentication)	
Authentication method	Mutual RSA
My identifier	My IP address
Peer identifier	Peer IP address
My Certificate	Structureality Site-to-Site VPN
Remote Certificate Authority	Structureality Enterprise Root
Phase 1 proposal (Algorithms)	
Encryption algorithm	256 bit AES-GCM with 128 bit ICV
Hash algorithm	SHA256
DH key group	14 (2048 bits)

OPNsense (c) 2014-2023 Deciso B.V.

Remote Desktop

- GUI-based remote terminal software
- Remote Desktop Protocol (RDP)
 - Connect to physical machines
 - RDP gateway to virtual desktops and apps
- HTML5/clientless
 - Access desktops and web applications from Internet via gateway to internal network
 - Browser support for canvas element plus WebSockets

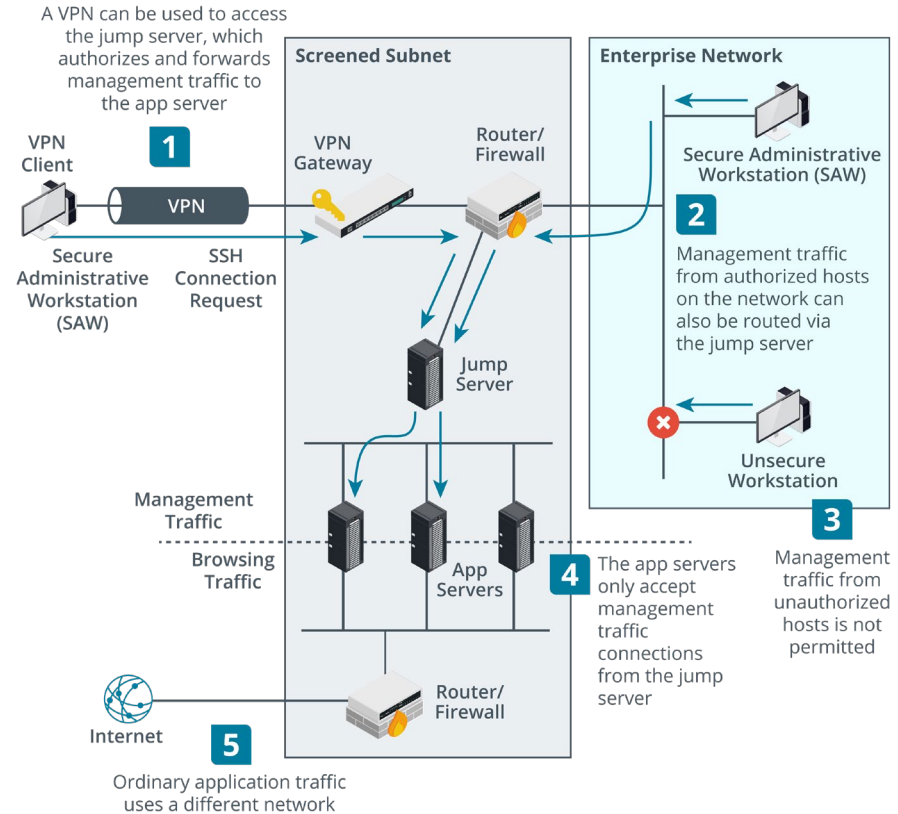
Secure Shell



- Remote administration with public key cryptography security
- Host key identifies server
- Client authentication
 - Username/password
 - Public key authentication
 - Kerberos
- Key management
- SSH commands
 - ssh versus scp (Secure Copy)

Out-of-band Management and Jump Servers

- Secure admin workstations (SAWs)
- Out-of-band (OOB) management
 - Serial/modem/console port
 - Virtual terminal
 - Separate cabling or VLAN isolation
- Jump servers
 - Single host accepts SSH or RDP connections from SAWs
 - Forwards connections to app servers
 - App servers only accept connections from jump server



Virtual Private Networks

- Remote access architecture
 - Tunneling, client-to-site remote access VPN, site-to-site VPN
- Transport Layer Security (TLS) tunneling
- Internet Protocol Security (IPSec) tunneling
- Internet Key Exchange
- Remote Desktop
- Secure Shell
- Out-of-band management and jump servers

CompTIA Security+ Exam SY0-701

Lesson 5



Summary

