Boston Network Users Group
March 7, 2017

Security Features of the Cisco Adaptive Security Appliance (ASA) Family of Devices

Jerry Joyce

Gerald R. Joyce, Ph.D.
https://www.linkedin.com/in/geraldrjoyce/

How my lab is set up

ASA security features similar to routers

ASA security features beyond those of routers

VPNs, including public /private keys

References:

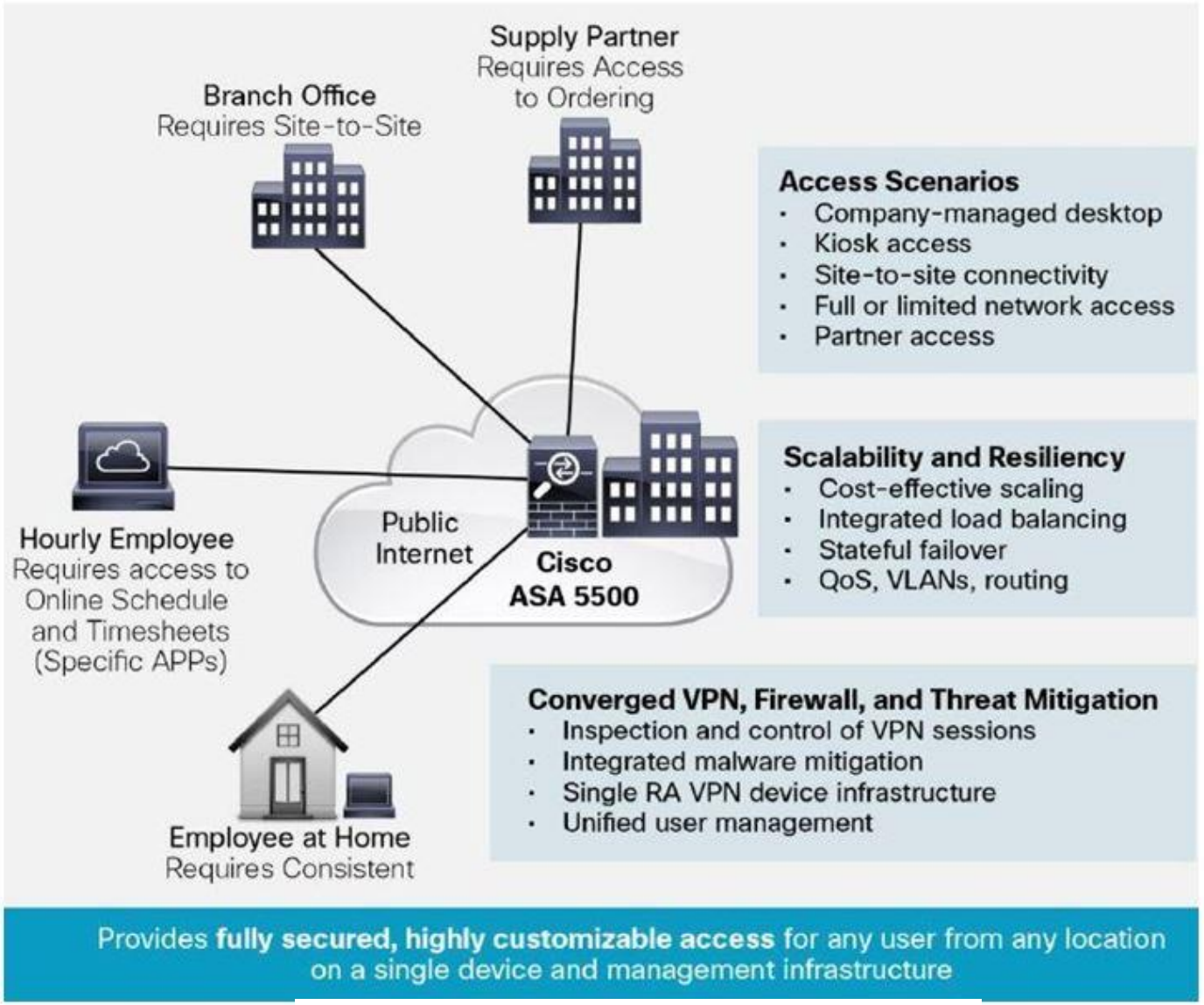
Cisco CCNA ICND2, Official Cert Guide, W Odem
Test 640-816 Switching and Routing
The test is out of date, but a very good book

Cisco CCNA Security, Official Cert Guide, O. Santos, J Stuppi
Test 210-260

Cisco ASA Configuration, R. Deal, Network Professional Library
Comprehensive manual

Cisco ASA Configuration for Accidental Administrators, D. Crawley
Brief but useful

ASA as Remote Access Device



Cisco Lab (basement)

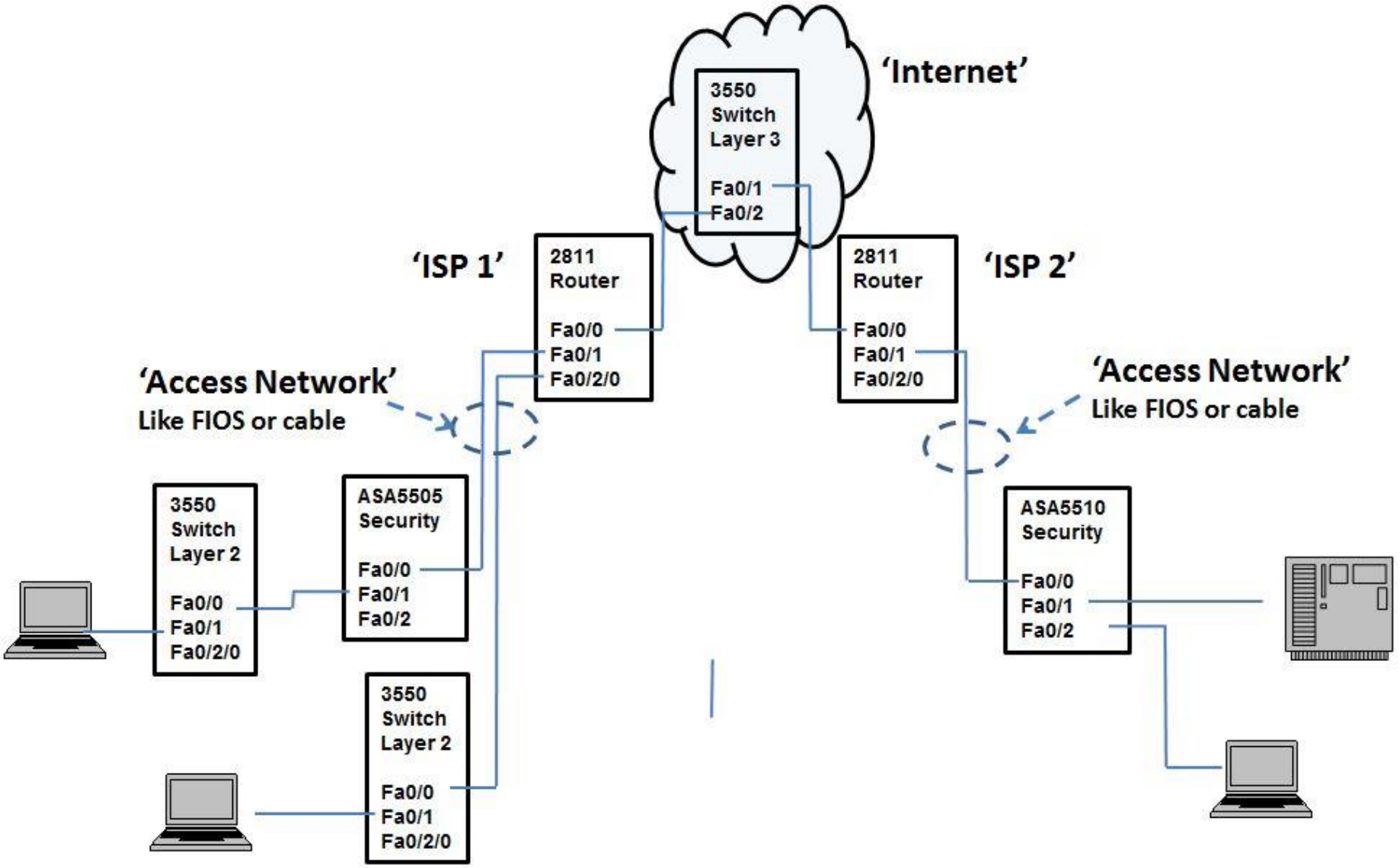
ASA 5510

2 ASA 5505's

'Internet' : 3550
Layer 3 switch
configured for routing

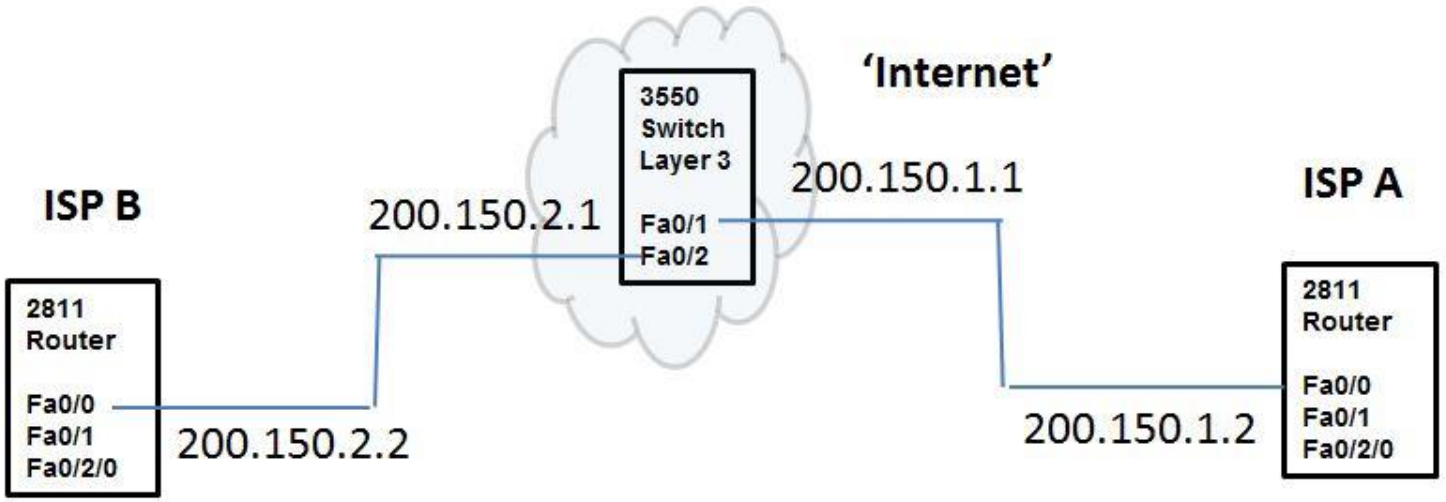
'ISP' A: 2811 router

'ISP' B: 2811 router


'Internet'
3550
Switch
Layer 3
Fa0/1
Fa0/2
'ISP 1'
2811
Router
Fa0/0
Fa0/1
Fa0/2/0
2811
Router
Fa0/0
Fa0/1
Fa0/2/0
'ISP 2'
'Access Network'
Like FIOS or cable
'Access Network'
Like FIOS or cable
3550
Switch
Layer 2
Fa0/0
Fa0/1
Fa0/2/0
ASA5505
Security
Fa0/0
Fa0/1
Fa0/2
ASA5510
Security
Fa0/0
Fa0/1
Fa0/2
3550
Switch
Layer 2
Fa0/0
Fa0/1
Fa0/2/0

ISP's connect over Internet via 'Public Addresses'

- This is the addressing in my lab



Public addresses, so-called 'outside network'
Private addresses: used for 'inside networks'

Generally used with subnetting

* = Wildcards for possible network addresses

0 = Minimum of last two bits left for host addresses

10.********.********.******00

172.16.********.******00 - 172.31.********.******00

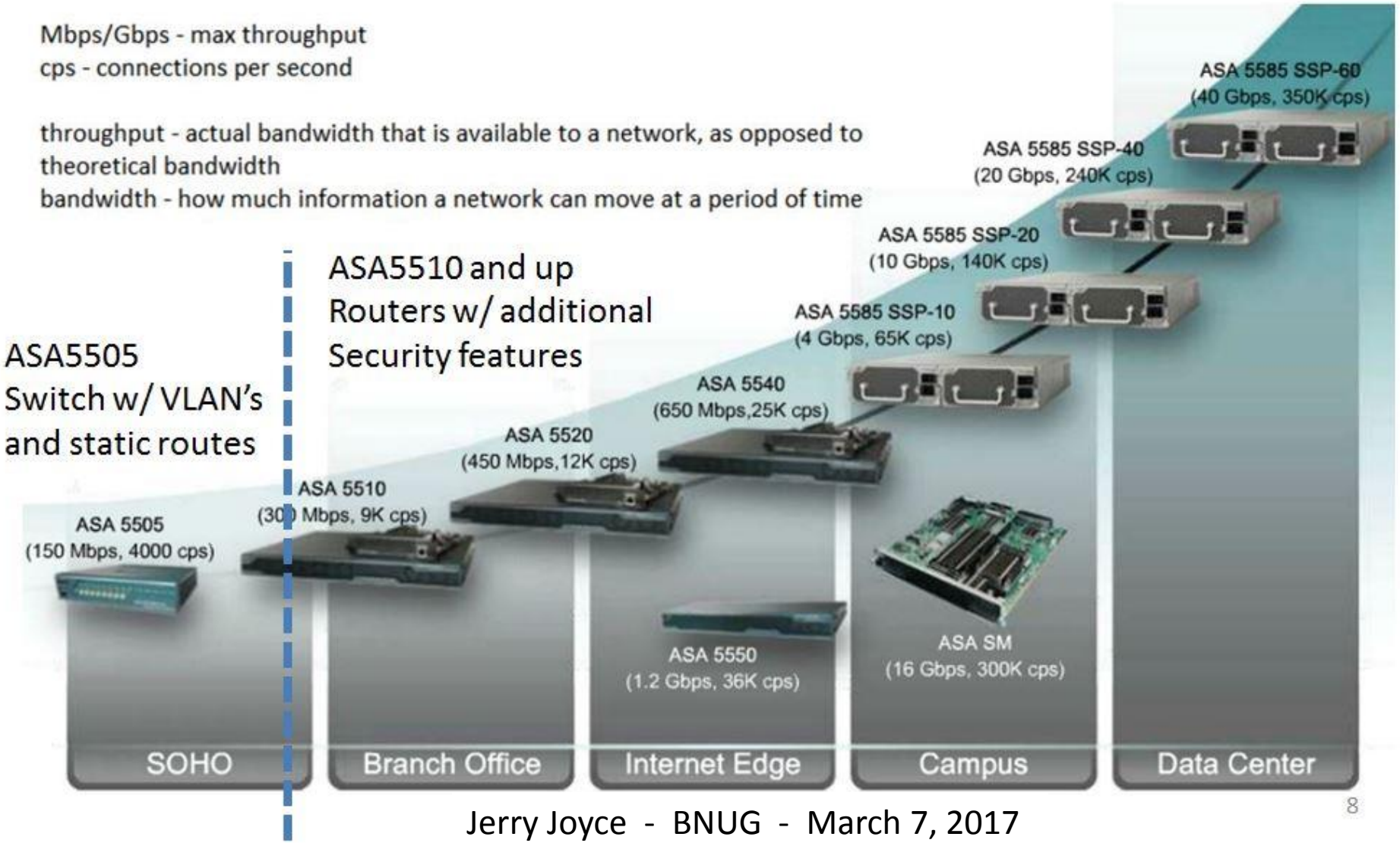
192.168.********.******00

RIP routing on interfaces, simple to use

Cisco Adaptive Security Appliance (ASA) Comparison

Mbps/Gbps - max throughput
cps - connections per second

throughput - actual bandwidth that is available to a network, as opposed to theoretical bandwidth
bandwidth - how much information a network can move at a period of time



Security Features Common to Routers

ASA 5505 is mainly a switch

- Needs to be connected to a router which defines the subnets
- Ports can be VLANs

ASA 5510 is a router

- Inside / Outside network interface
- Routing protocols include RIP, OSPF, EIGRP

Router security features

- Network address translation (NAT) between inside network and outside network
- Access Control Lists to filter packets at various interfaces. Packets that do not match an ACL will be dropped

ISP's connect over Internet via 'Public Addresses'

Public addresses, so-called 'outside network'
Private addresses: used for 'inside networks'

Class A and B networks generally used with subnetting

* = Wildcards for possible network addresses

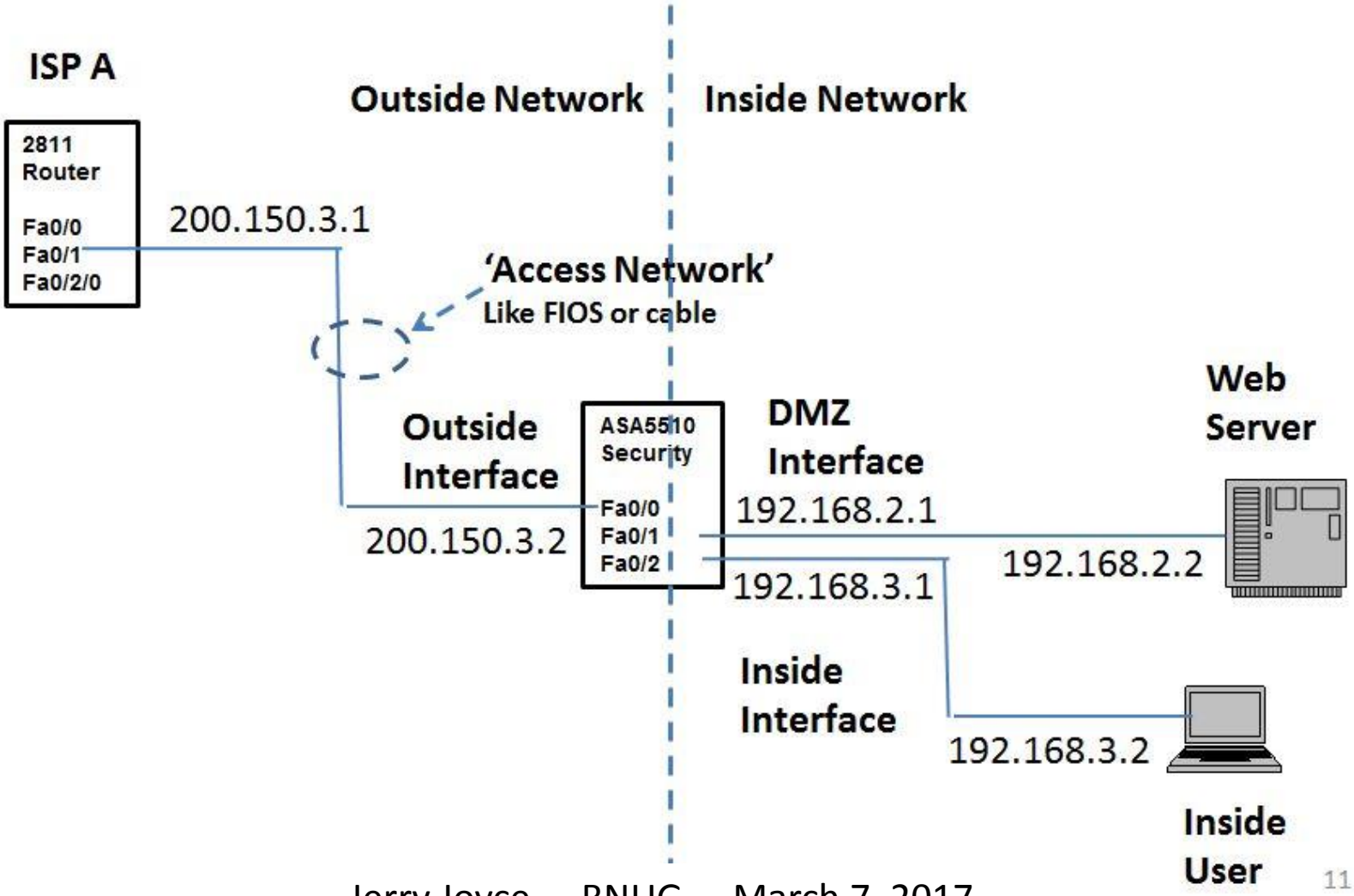
0 = Minimum of last two bits left for host addresses

10.0.0.0 is the usual definition of private class A network
10.********.********.******00 with subnetting

172.16.0.0 – 172.31.0.0 is usual definition off private class B network
172.16.********.******00 - 172.31.********.******00 with subnetting

192.168.0.0 is usual definition of private class C network
192.168.********.******00 with subnetting

ASA5510 as Inside / Outside Network Boundary



What is Network Address Translation?

Applies to packets passing between the outside interface(s) on the 'outside network' and interfaces on the 'inside network' such as DMZ interface and Inside interface

- The inside network hosts are referred to in the IP header with 'private addresses' while the packet is in the 'inside network'
- The same inside network hosts are referred to in the IP header with 'global' (meaning public or routable) addresses while the same packet is on the outside network
- The relevant source or destination IP addresses (that reference the inside network hosts) have to be changed when the packet passes between outside and inside networks.

Syntax for NAT Configuration

(from show running-config)

```
!
interface Ethernet 0/0
 ip address 10.1.1.3   255.255.255.0
 ip nat inside
!
 interface Ethernet 0/1
 ip address 200.1.1.251   255.255.255.0
 ip nat outside
!
ip nat pool xyxyxy  200.1.1.1  200.1.1.2  netmask 255.255.255.252
ip nat inside source list 1 pool xyxyxy
!
!
access-list 1 permit 10.1.1.1
access-list 1 permit 10.1.1.2
!
```

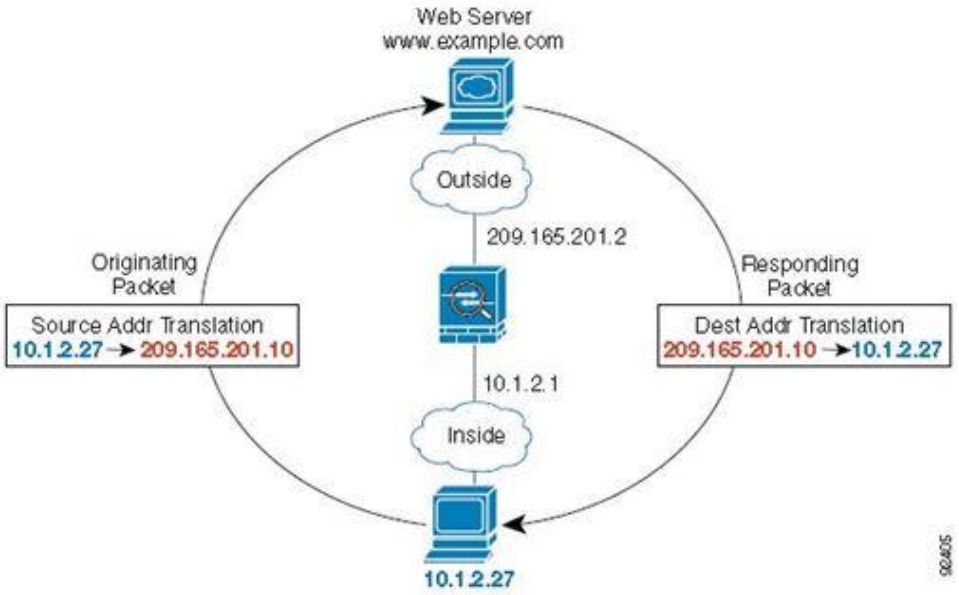
Define NAT for iterface Ethernet0/0

Define pool of public addresses

Define list of allowed private addresses

Example of Network Address Translation

Figure 15-1 NAT Example



- Typical NAT scenario, with a private network on the inside.
- When the inside user sends a packet to a web server on the Internet, the local source address of the packet is changed to a routable global address.
- When the web server responds, it sends the response to the global address, and the security appliance receives the packet. The security appliance then translates the global address to the local address before sending it on to the user.

Security and other Benefits of NAT

- Use private addresses on inside networks. Private addresses are not routable on the Internet.
- NAT hides the local addresses from other networks, so attackers cannot learn the real address of a host.
- NAT can resolve IP routing problems by supporting overlapping IP addresses.
- Network scaling: Similar internal addressing designs can be used across multiple locations. Than NAT definitions can translate to non-overlapping public addresses.
- Easier to switch ISP's (i.e., public addressing) while keeping inside addressing (local network design) the same

Access Control Lists (ACL's), powerful packet filtering at interfaces

Figure 8-5 *Extended ACL Syntax with Port Numbers Enabled Using Protocol TCP or UDP*

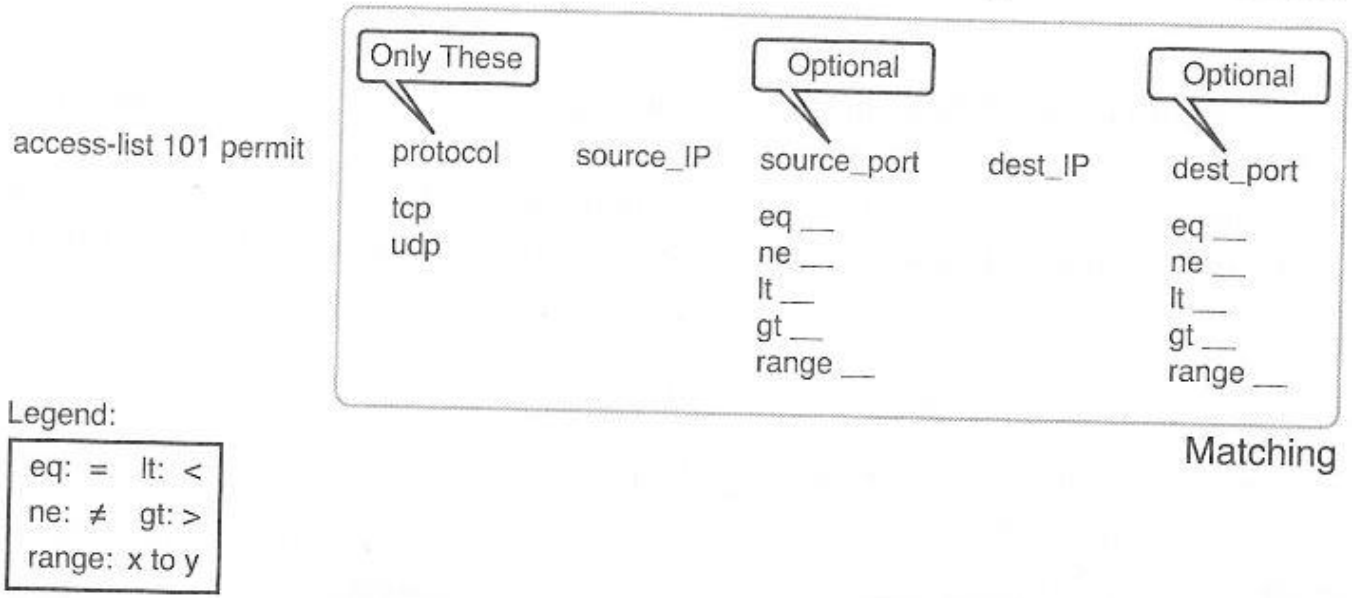
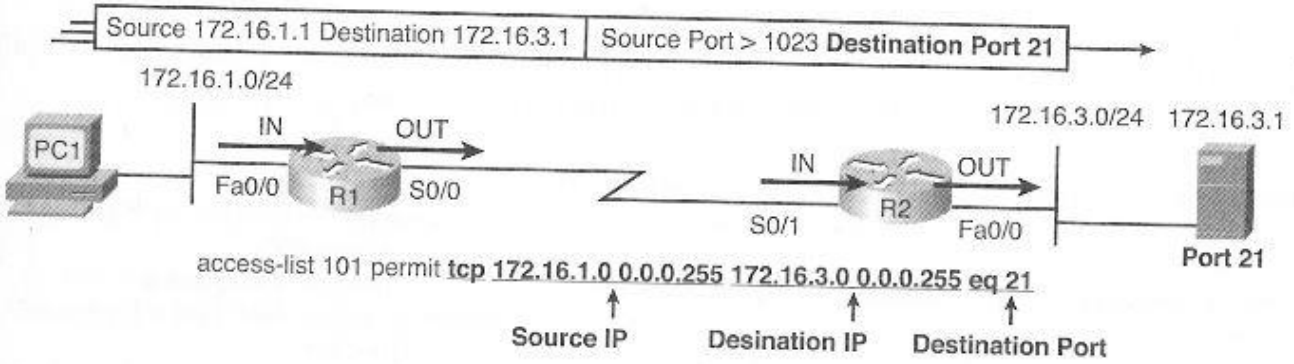


Figure 8-6 *Filtering Packets Based on Destination Port*



Access Control Lists (ACL's), powerful packet filtering at interfaces

Table 8-3 *Popular Applications and Their Well-Known Port Numbers*

Port Number(s)	Protocol	Application	access-list Command Keyword
20	TCP	FTP data	**ftp-data**
21	TCP	FTP control	**ftp**
22	TCP	SSH	—
23	TCP	Telnet	**telnet**
25	TCP	SMTP	**smtp**

Port Number(s)	Protocol	Application	access-list Command Keyword
53	UDP, TCP	DNS	**domain**
67, 68	UDP	DHCP	**nameserver**
69	UDP	TFTP	**tftp**
80	TCP	HTTP (WWW)	**www**
110	TCP	POP3	**pop3**
161	UDP	SNMP	**snmp**
443	TCP	SSL	—
16,384 – 32,767	UDP	RTP-based voice (VoIP) and video	—

Security Features of ASA's that go beyond Standard Routers

Security Levels of Interfaces
- Each interface is defined with a security level between 0 and 100
- By default packets are not allowed to pass from lower to higher security levels, or even between equal security levels
- Explicit permission by ACL, or VPN required to pass packet

Stateful set-up of connections
- Cut-through packet forwarding

Filtering services

Security Service Modules

Virtual Private Networks
- Network to Network
- Network to remote device or user
- Multiple methods to configure
- Includes pubic key infrastructure

ASA5510 Running-configuration

```
asa5510#
asa5510#
asa5510# show running-config
: Saved
:
: Serial Number: JMX1506L07T
: Hardware:   ASA5510, 1024 MB RAM, CPU Pentium 4 Celeron 1600 MHz
:
ASA Version 9.1(7)11
!
hostname asa5510
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Ethernet0/0
 nameif outside
 security-level 0
 ip address 200.150.3.2 255.255.255.0
!
interface Ethernet0/1
 nameif dmz
 security-level 50
 ip address 192.168.2.1 255.255.255.0
!
interface Ethernet0/2
 nameif inside
 security-level 100
 ip address 192.168.3.1 255.255.255.0
!
```

By default, packets will only pass from Higher security-level interface to Lower security-level interface

Access-control-list (ACL) or VPN required for anything else

Cut-through-proxy (CTP) performance improvement over traditional proxy-server

A **proxy server** is a server that acts as an intermediary for requests from clients seeking resources from other servers.

- A traditional proxy server suffers because it analyzes every packet

The security appliance cut-through proxy challenges a user initially at the application layer and authenticates against standard **AAA** servers or the local database.

- After the security appliance authenticates the user, it shifts the session flow, and all traffic flows directly and quickly between the source and destination while maintaining session state information. (config guide)

Authentication, Authorization, Accounting

As the first process, authentication provides a way of identifying a user

- Typically by via user name and password.
- The AAA server compares a user's authentication credentials with other user credentials stored in a database.

Next a user must gain authorization for doing certain tasks.

- The process of enforcing policies: determining what types or qualities of activities, resources, or services a user is permitted.
- Usually, authorization occurs within the context of authentication. Once you have authenticated a user, they may be authorized for various types of access or activity.

Last is accounting, which measures the resources a user consumes during access.

- The amount of system time or the amount of data a user has sent and/or received during a session.
- Logging of session statistics and usage
- Used for authorization control, billing, trend analysis, resource utilization, and capacity planning activities.

AAA Process in ASA

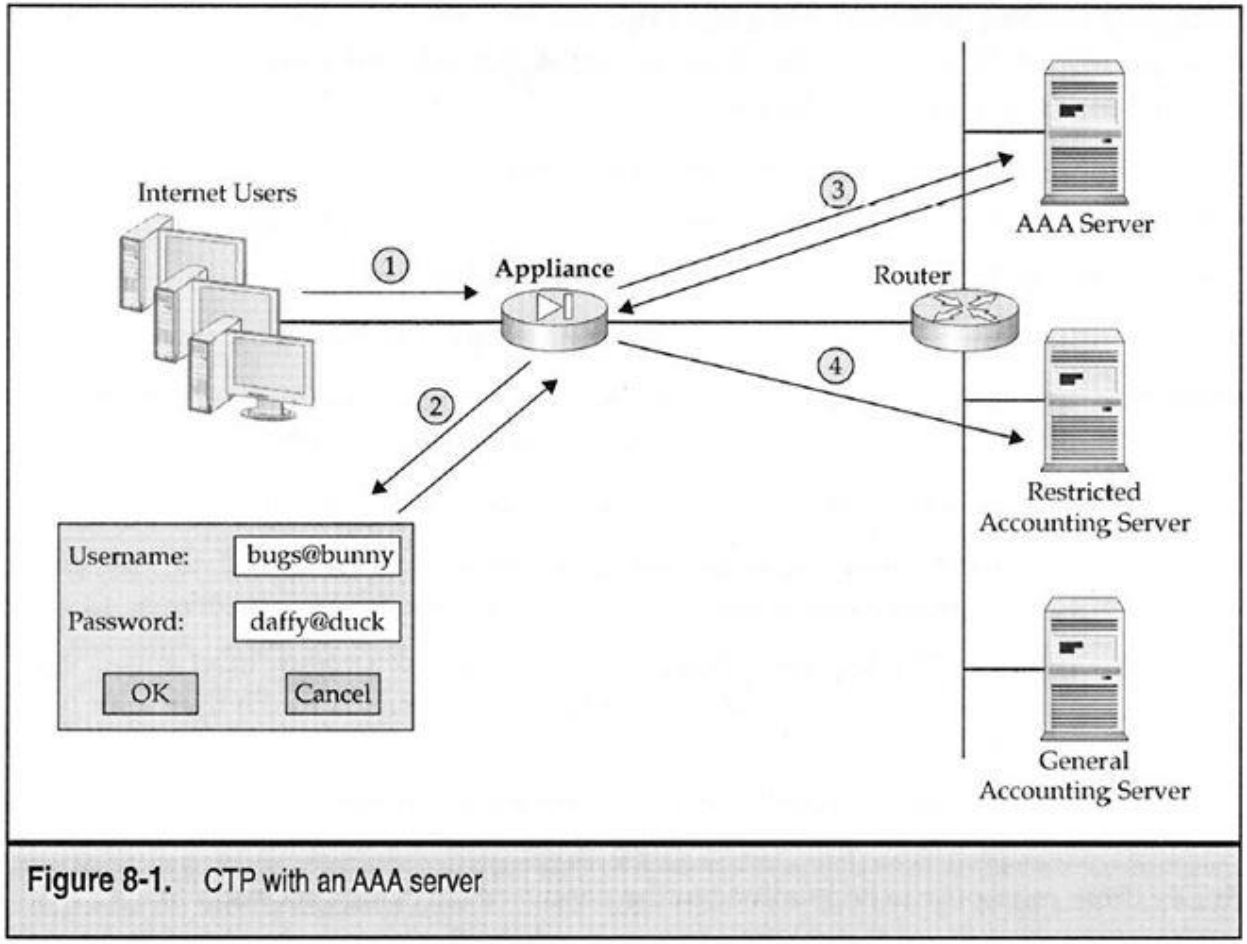


Figure 8-1. CTP with an AAA server

RADIUS (DIAMETER) and TACACS+

Secure transport needed between the ASA security appliance and the AAA server.

RADIUS

- Owned by Lucent but essentially open now
- Uses UDP transport
- Only encrypts the user password, everything else is clear
- Developed for ISPs so robust accounting system

TACACS+

- Originally developed by Defense Dept but now proprietary to Cisco
- Uses TCP transport, single connection for entire transaction
- Encrypts the entire payload in security packets, more secure

ASA Filtering Services

Filter ActiveX objects or Java applets, that may pose a security threat

ActiveX Objects Filtering

- Security risks because they can contain code intended to attack hosts and servers on a protected network.
- ActiveX objects can be inserted in a web page or other application. They include custom forms, calendars, or any of the extensive third-party forms for gathering or displaying information.
- ActiveX creates many potential problems for network clients including causing workstations to fail, introducing network security problems, or being used to attack servers.

Filtering Java Applets

- Prevent Java applets from HTTP traffic passing through the firewall.
- These are security risks because they can contain code intended to attack hosts and servers on a protected network.
- Filters out Java applets that return to the security appliance from an outbound connection.
- The user still receives the HTML page, but the web page source for the applet is commented out so that the applet cannot execute.

Filtering URLs and FTP Requests with an External Server

When filtering is enabled and a request for content is directed through the security appliance, the request is sent to the content server and to the filtering server at the same time.

- If the filtering server allows the connection, the security appliance forwards the response from the content server to the originating client.
- If the filtering server denies the connection, the security appliance drops the response and sends a message or return code indicating that the connection was not successful.

The server runs one of the following Internet filtering products:

- Websense Enterprise for filtering HTTP, HTTPS, and FTP.
- Secure Computing SmartFilter (formerly N2H2) for filtering HTTP, HTTPS, FTP, and long URL filtering.

Security Services Module (SSM) Blade for ASA5500 series

(Source: Cisco marketing material)

Security Services Module Features

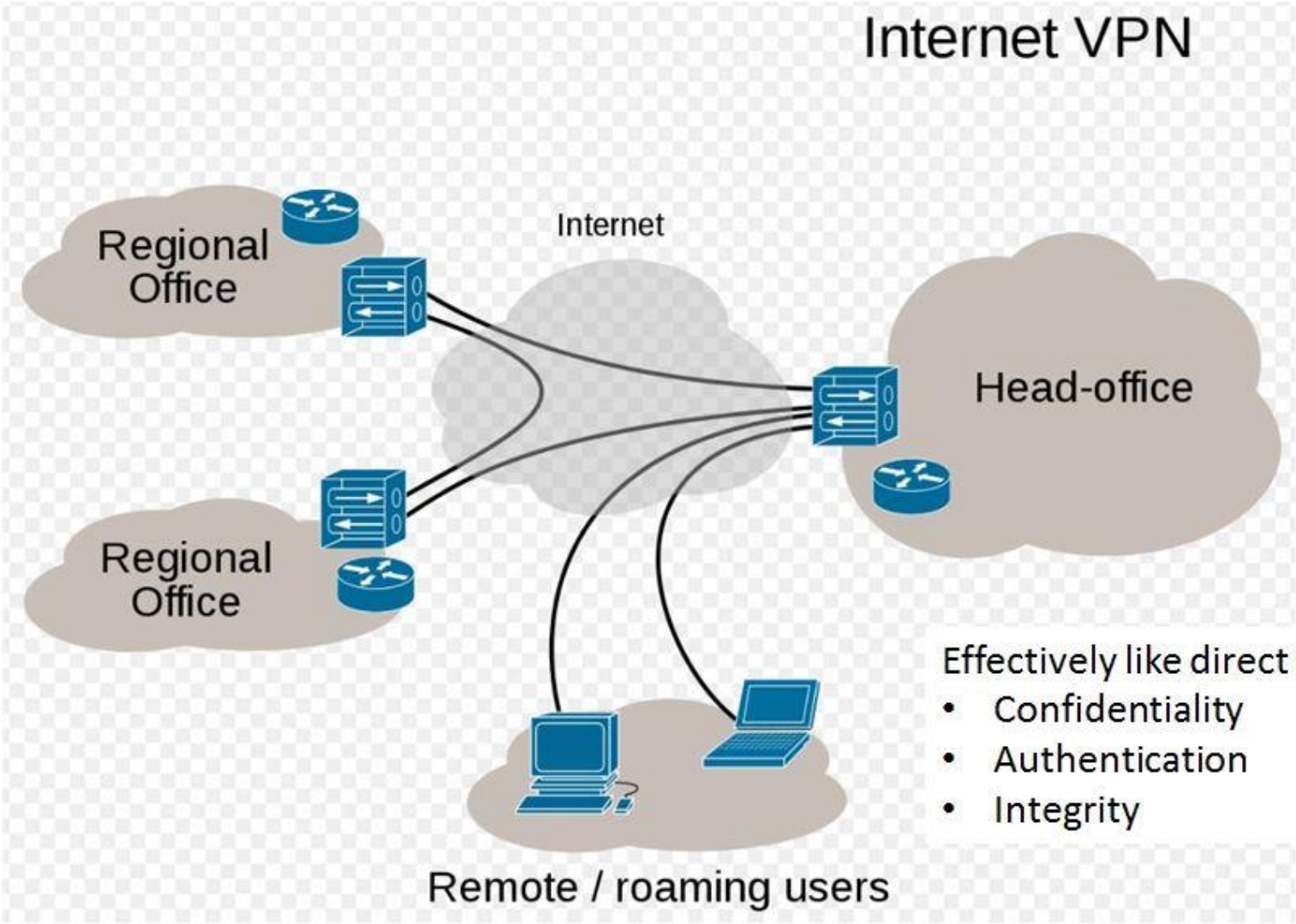
Advanced Inspection and Prevention

- Part of intrusion prevention system (IPS)
- The adaptive security appliance diverts packets to the AIP SSM just before the packet exits the egress interface or before VPN encryption
- Detailed inspection of traffic in Layers 2 through 7.
- Comprehensive protection of network by collaborating with other network security resources

Content Security and Control

- Antivirus, anti-spyware, file blocking, anti-spam, anti-phishing, URL blocking and filtering, and content filtering
- Prevents malicious code from entering and propagating across the network
- Anti-spam technology that removes the vast majority of unsolicited e-mail before it gets to the mail server

A VPN is a secure connection across a network (such as the Internet) that appears as a private connection.



https://en.wikipedia.org/wiki/Virtual_private_network

A VPN is a secure connection across a network (such as the Internet) that appears as a private connection.

Privacy → encryption

- Private / Public Keys…..asymmetric
  Private key encrypt and public key decrypt
  Strongest but most computationally intensive to use
- Shared Secret ……symmetric
  Shared secret used for both encrypt and decrypt
  Strong but computationally more practical

Authentication → digital signature

- Proves the message came from person you think sent it
- Uses private / public keys

Integrity → Message is unchanged

- Based on hash algorithm
- One bit change to message will change hash
- Computationally efficient
- The hash is short…this is NOT encryption…one way only

Internet Security Association Key Management Protocol (ISAKMP) RFC 2408

Authentication

- An important step in establishing secure network communications is authentication of the entity at the other end of the communication.
- Digital signatures are public key based strong authentication mechanisms.
- Each entity requires a public key and a private key.
- Certificates are an essential part of a digital signature authentication

Certificate authority (CA)

- Each communicating entity generates public / private key pair
  - Requests digital certificate from CA
- CA issues the digital certificate
  - Certifies the owner of a public key.
- CA is trusted by both the key owner and the party receiving message.
- Public-key (PKI) schemes used for VPN's and https

https://tools.ietf.org/html/rfc2408
https://en.wikipedia.org/wiki/Certificate_authority

Internet Security Association Key Management Protocol (ISAKMP) RFC 2408

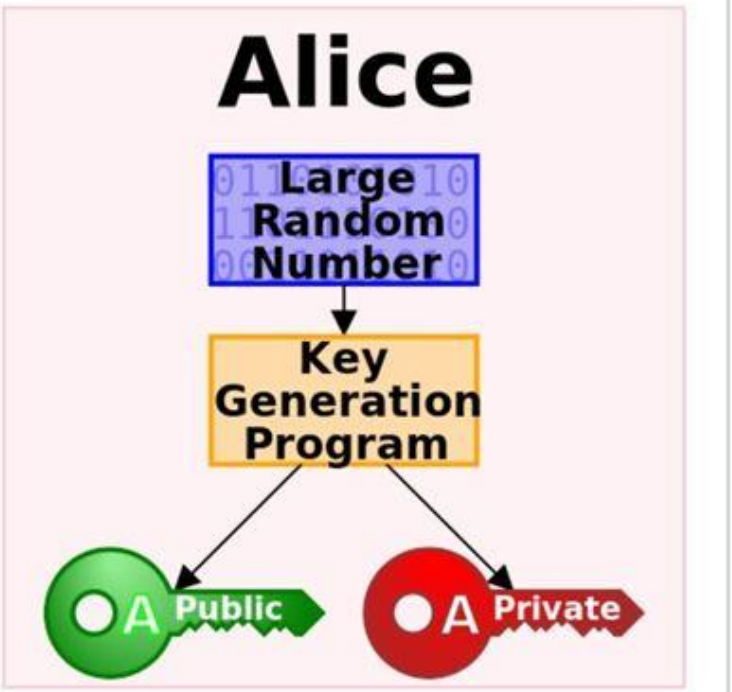
Phase 1,

- Phase 1 supports high security asymmetric encryption to peer
  - Public/ private keys usually
  - Also pre-shared key (manually configured)
- This encryption is then used to protect future negotiations

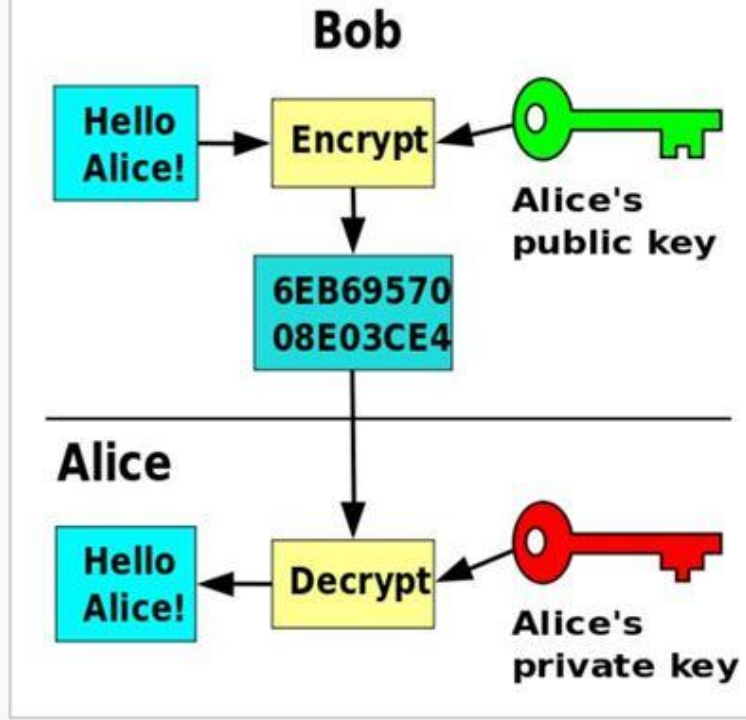
Phase 2

- Additional SA's are set up between peers
- These SA's can use other security protocols to set up more efficient encryption/decryption keys
  - Difffie-Hellman key exchange
  - Pre-shared keys (manually configured)
- These SA's can be used for many message / data exchanges.

Public & Private Keys → Asymmetric Encryption



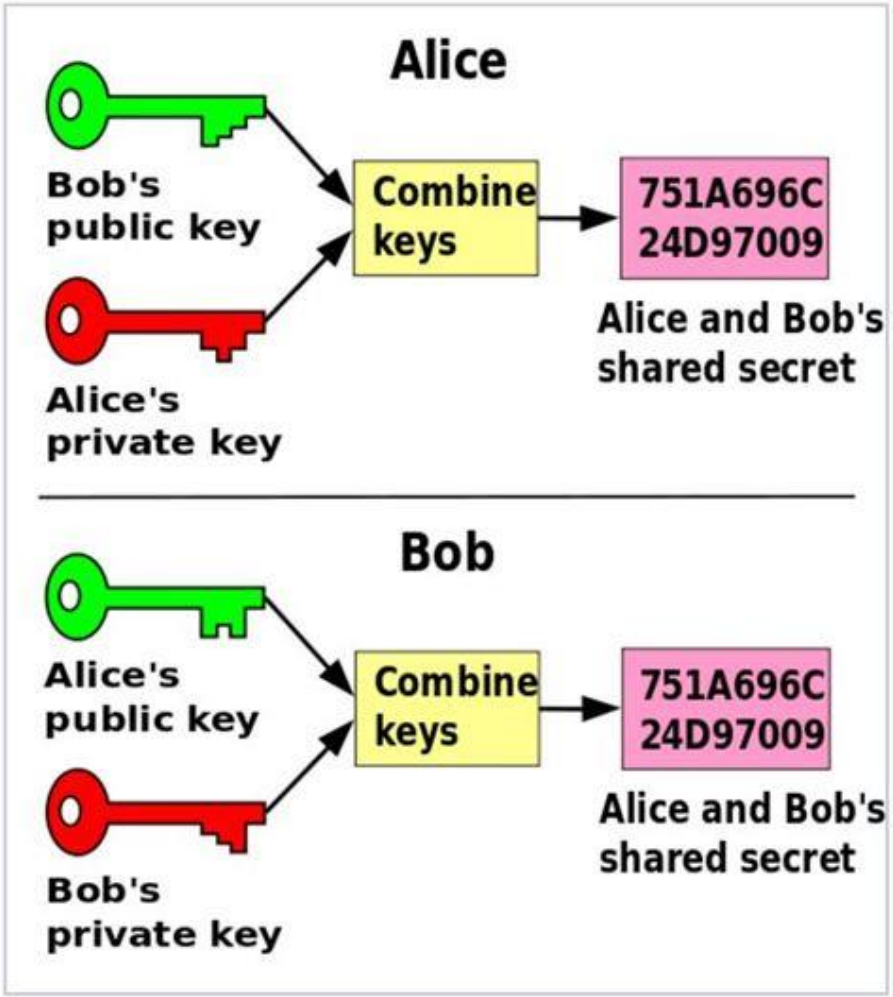
An unpredictable (typically large and random) number is used to begin generation of an acceptable pair of keys suitable for use by an asymmetric key algorithm.



In an asymmetric key encryption scheme, anyone can encrypt messages using the public key, but only the holder of the paired private key can decrypt. Security depends on the secrecy of the private key.

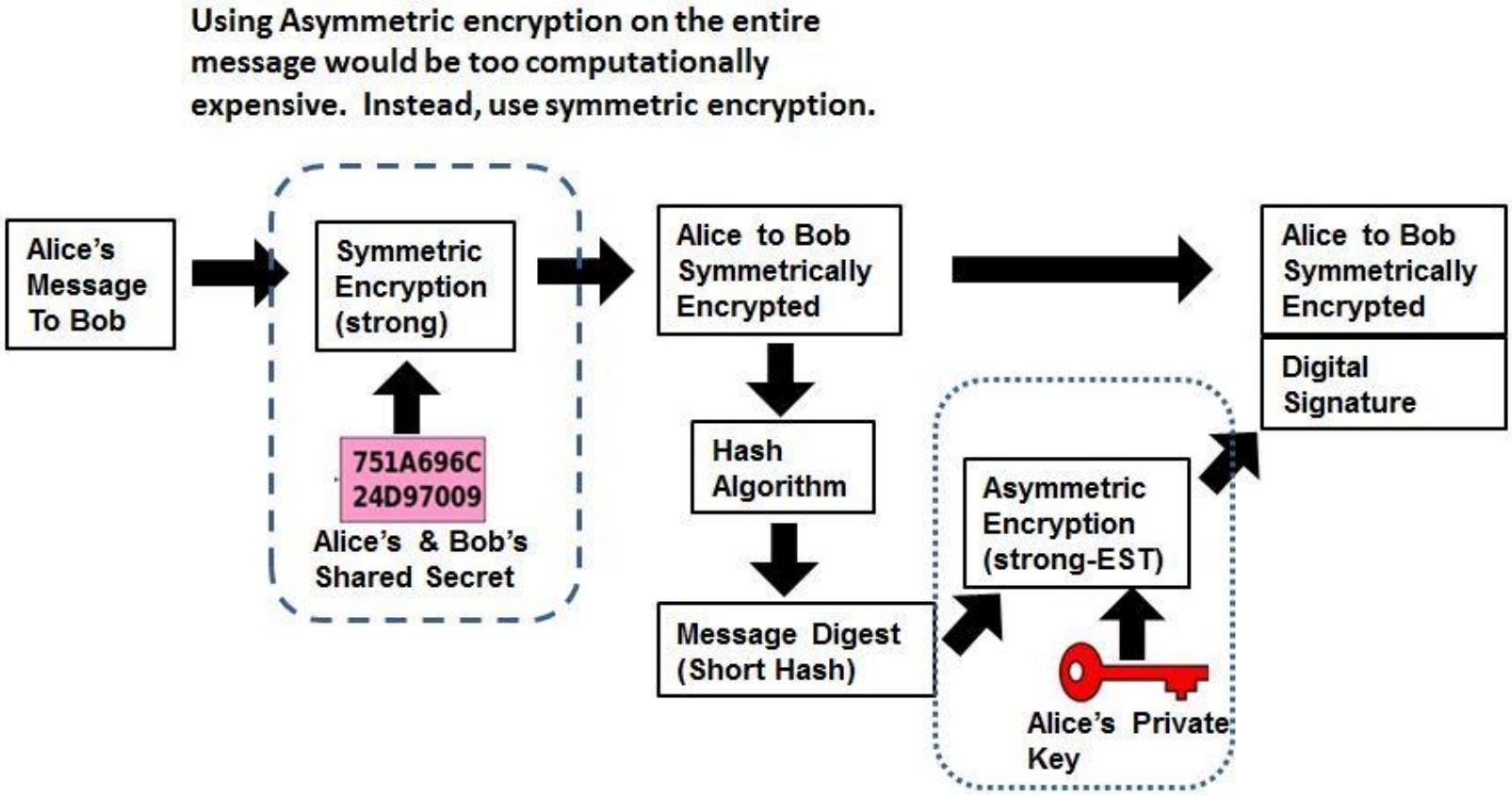
- Alice creates her private and public keys. No one else knows the Alice's private key.
- Anyone (e.g., Bob) can know Alice's public key (e.g., via a Certificate Authority)
- Asymetric encryption is highly secure but computationally expensive
- *Recall: Phase 1 negotiations between peers and digital signatures*
- https://en.wikipedia.org/wiki/Public-key_cryptography

Diffie-Hellman Symmetric Key Exchange

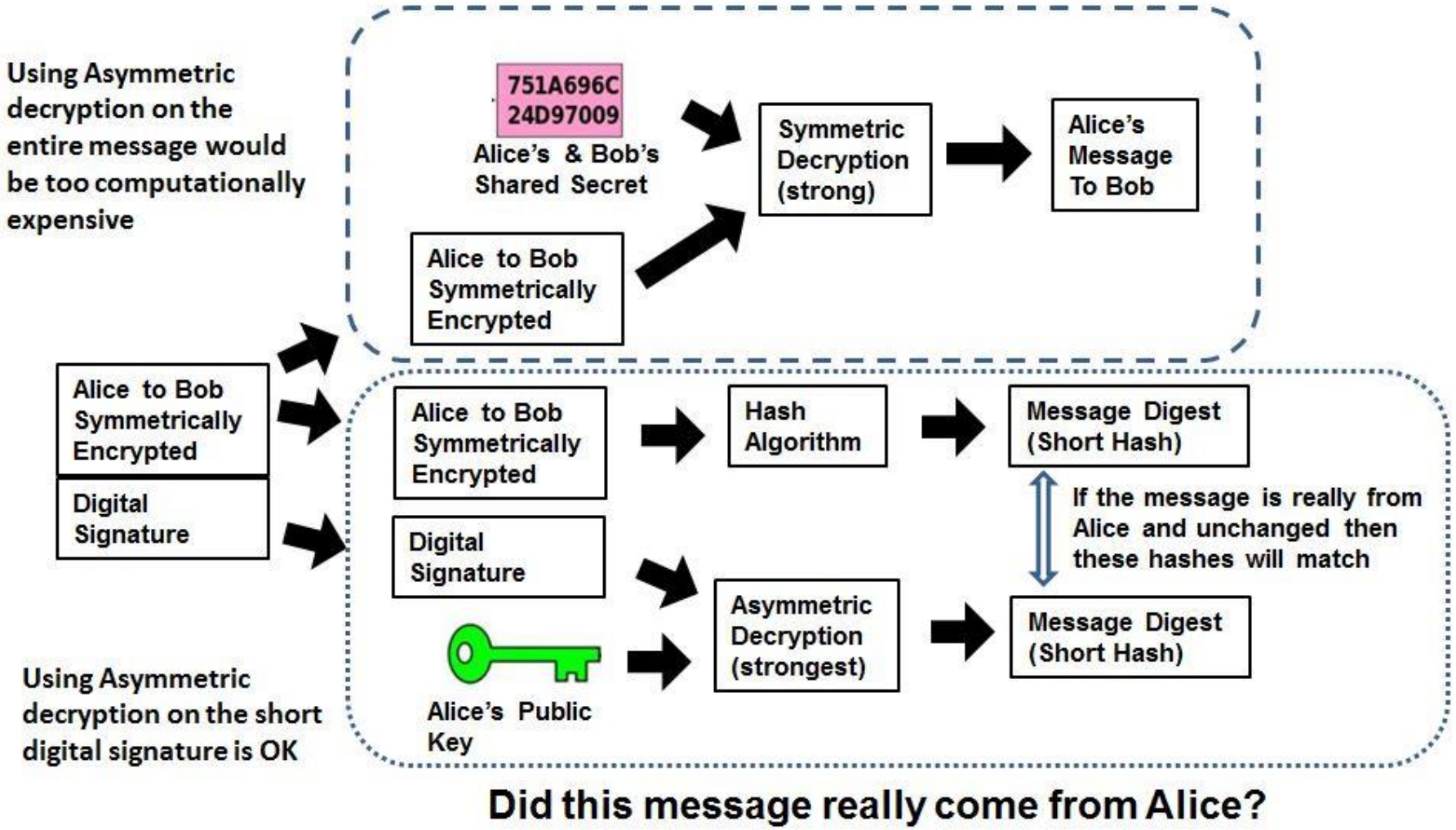


- Each peer has their own private key and the authenticated public key of the other party
- Each combines the pair of keys with the Diffie-Hellman algorithm
- Each generates the same shared secret that can be used for encrypting and decrypting
- Symmetric encryption is less computationally expensive than asymmetric encryption
- *Useful for entire duration of data exchange over secure channel*
- Called Phase-2
- https://en.wikipedia.org/wiki/Public-key_cryptography

Alive encrypts and signs Message to Bob



Bob decrypts Message from Alice



ASA's in a VPN must Create and Manage Tunnels

Tunneling uses a public TCP/IP network to create secure connections

- ASA to ASA network to network
- Host to ASA remote access
- Each secure connection is called a tunnel.

The ASA becomes a bidirectional tunnel endpoint.

- Receive plain packets from the private network & encapsulate them.
- Send packets to the other end of the tunnel where they are un-encapsulated and sent to their final destination.
- Also receive encapsulated packets from the public network, un-encapsulate them
- and send them to their final destination on the private network.

ASA's have to build and manage tunnels between the endpoints (i.e. peers)

- Negotiate tunnel parameters
- Establish tunnels
- Authenticate users
- Manage security keys
- Encrypt and decrypt data
- Manage data transfer across the tunnel
- Manage data transfer inbound and outbound as a tunnel endpoint or router

Method 1: IP Security (Ipsec)

IPsec for LAN-to-LAN VPN connections

- Option of IPsec for client-to-LAN VPN connections.
- In IPsec terminology, a *peer* is a remote-access client or another secure gateway.
- Peers create security associations (SAs)

IPsec LAN-to-LAN connections, the security appliance can function as initiator or responder

IPsec client-to-LAN connections, the security appliance functions only as responder.

Initiators propose SAs; responders accept, reject, or make counter-proposals

IPsec relies on ISAKMP to build an IPsec security association

- Phase 1 creates the first tunnel, which protects later ISAKMP negotiation messages.
  - Uses asymmetric public/private key encryption which is computationally expensive
- Phase 2 creates the tunnel that protects data.
  - More efficient encryption such as preshared keys or Diffie-Hellman
  - Authentication: Hash algorithm, digital signatures

IPsec VPN using ASA Command Line

Create an ISAKMP policy, which includes the following:

- Complicated commands

An authentication method, to ensure the identity of the peers.

- Challenge / response
- Digital certificate
- Pre-shared keys

An encryption method, to protect the data and ensure privacy.

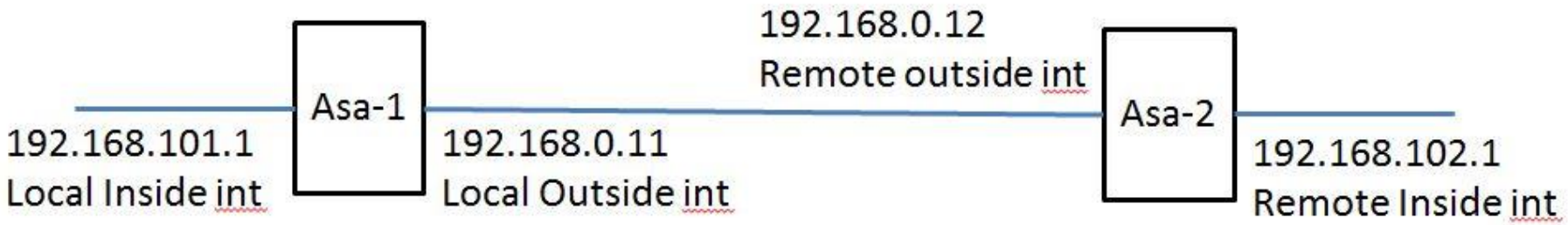
- 3DES
- Advanced Encryption Standard

A Hashed Message Authentication Codes (HMAC) for identity of the sender, and to ensure that the message has not been modified in transit.

A Diffie-Hellman group to determine the strength of the encryption-key-determination algorithm.

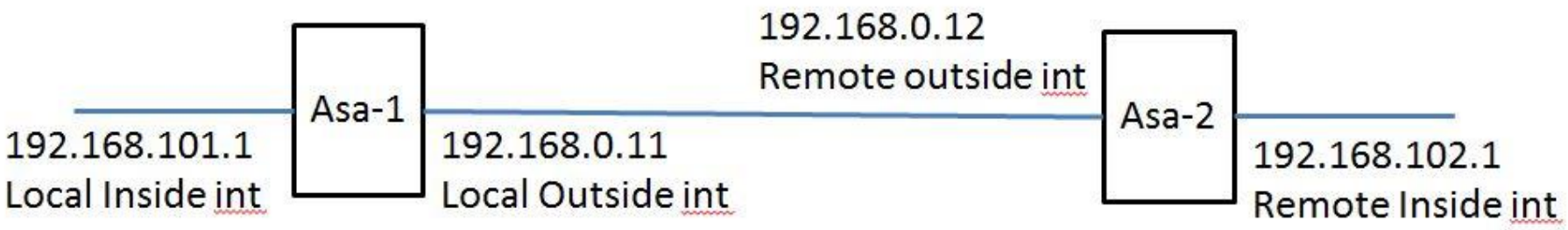
- The security appliance uses this algorithm to derive the encryption and hash keys

IPsec VPN using ASA Command Line



1. ciscoasa1(config) # crypto isakmp enable outside
   enable ISAKMP on the outside interface of ASA-1
2. ciscoasa1(config) # access-list_1_cryptomap permit ip 192.168.101.0 0.0.0.255 192.168.102.0 0.0.0.255
   An ACL for traffic from ASA-1 inside ip subnet to ASA-2 inside ip subnet
3. ciscoasa1(config) # tunnel-group 192.168.0.12 type ipsec-l2l
   (ie, lan 2 lan) tunnel-group between outside interfaces on the two ASA's
4. ciscoasa1(config) # tunnel-group 192.168.0.12 type ipsec-attributes
5. ciscoasa1(config-tunnel-ipsec) #pre-shared-key p@ss5678
6. ciscoasa1(config-tunnel-ipsec) # isakmp keep-alive threshold 10 retry 2
7. ciscoasa1(config-tunnel-ipsec) #exit

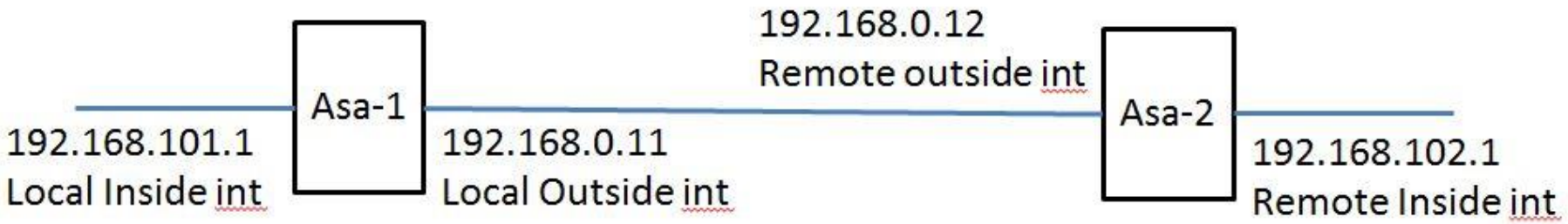
IPsec VPN using ASA Command Line



Configure Phase 1

8. ciscoasa1(config) # crypto isakmp policy 10 authentication pre-share
   here use pre-shared keys
9. ciscoasa1(config) # crypto isakmp policy 10 encryption aes
   use aes (advanced encryption standard) for encryption
10. ciscoasa1(config) # crypto isakmp policy 10 hash sha
    choose the hashing algorithm
11. ciscoasa1(config) # crypto isakmp policy 10 group 2
    diffie-hellman group 2

IPsec VPN using ASA Command Line



Configure Phase 2

12. ciscoasa1(config) # crypto ipsec transform-set ESP-AES-SHA esp-aes esp-sha-hmac
13. ciscoasa1(config) # crypto map outside_map 1 match address outside_1_cryptomap
14. crypto map outside_map 1 set pfs group2
15. crypto map outside_map 1 set peer 192.168.0.12
16. crypto map outside_map 1 set transform-set ESP-AES-SHA
17. crypto map outside_map interface outside

Method 2. SSL VPN ….. Between main site ASA (as server) and remote client (browser)

SSL VPN Client (SVC) VPN gives remote users the benefits of an IPSec VPN client without excessive configuration

- Uses the **Secure Sockets Layer** (SSL) that is already present on the remote computer (browser) and ASA
- remote user enters the IP address of a WebVPN interface on the ASA
- displays the WebVPN login screen
- If user satisfies the login authentication and authorization
- ASA downloads the SVC to the remote computer.
- the SVC installs and configures itself