Advanced Topics in Enterprise VPNs and PKI

Session 2403
Agenda

• IPSec Brief Overview
• PKI and DigitalCertificates
• Deploying IPSec in the Enterprise
• Multiservice and IPSec
**IPSec Algorithms**

**Authentication Header**
- Router
- IP HDR
- AH
- Data
- Firewall

**Encapsulating Security Payload**
- Router
- IP HDR
- ESP
- Data
- Firewall

**IPSec Modes**

**Tunnel Mode**
- IP HDR
- DATA
- New IP HDR
- IPSec HDR
- IP HDR
- DATA
- Encrypted

**Transport Mode**
- IP HDR
- IPSec HDR
- DATA
- Encrypted
IKE

- Negotiates policy to protect communication
- Authenticated Diffie-Hellman key exchange
- Negotiates (possibly multiple) security associations for IPSec
- A flavor of ISAKMP/Oakley for IPSec
- Provides PFS
- Pre-shared keys, digital certificates

PKI and Digital Certificates
Outline

- Digital Certificate Overview. What is PKI and PKIX?
- Algorithms and Tools
- PKI Deployment Considerations
- SCEP Overview and a Working Example
- PKI and the IETF

Why Digital Certificates?

- Scalability
- Security
- Trusted validation of parties
- Transmission and storage can be insecure
- Changes can be detected
- Can provide config and permissions
What Is a Digital Certificate?

- A data structure that binds a public key value to a subject
- Binding is achieved by a trusted CA verifying the subject’s identity and digitally signing the certificate
- Has a limited lifetime which is checked by the relying party along with the signature

What Is a Public-Key Infrastructure?

- Provides trusted and efficient key and public key certificate management
- Enables authentication, non-repudiation and confidentiality
- Used by protocols such as S/MIME, TLS and IPSec
What Is PKIX?

- PKI specifications for the Internet using PKCs
- Public key infrastructure for X.509
- Current versions:
  - X.509 v3 PKC
  - version 2 CRLs
- Defines data formats and procedures for the issuing of certificates by CAs
Certificate Life Cycle and Management—PKIX

Initialization

Certification

Useful Life

Expiration

Revocation

X.509v3 Certificate

- Binds user identity (subject name) to a public key via signature
- Issuer (CA) signs cert
- Note cert has defined lifetime
- Identifies which signature algorithm was used to sign cert
- Extension fields allow other information to be bound to cert (e.g., subject’s clearances)
PKI Components—CAs

- Certificate Authority (CA) verifies identity
- CA signs digital certificate containing device’s public key
- Revokes Certificates
- Verisign on-site, Entrust PKI, Netscape CA, Microsoft CA

PKI Components—RAs

- Interface between the CA and end entity
- Perform administrative tasks on behalf of the CA
- May have many RAs to one CA (e.g. administration for specific groups)
Other PKI Components

- End-entity (EE) — a subject of a certificate, not a CA
- Relying party — a user or agent that relies on the data in the certificate

Other PKI Components

- Root CA — a CA directly trusted by an EE. Can be the top of a hierarchy
- Subordinate CA — not the root CA for an EE, but may chain from an EE to a root CA
- Subject — The EE named in a certificate. Mostly represented by DNS names or IP addresses
Certificate Revocation List

- List of revoked certificate’s serial numbers signed by CA
- Stored on CA or directory service
- Time-stamped and frequently updated

Interactions Between PKI Components

- CRLs and Certs
- DirSrv
- Operational and Management Transactions
- End Entity
- Management Transactions
- PKI Users
- Publish Certs
- RA
- Publish Certs and CRLs
- CA
- PKI Management Entities
- CA Users
- Management Transactions
Digital Signatures

- Entity authentication
- Data origin authentication
- Integrity
- Non-repudiation

Key Sizes

<table>
<thead>
<tr>
<th>Secret Key</th>
<th>Public Key</th>
</tr>
</thead>
<tbody>
<tr>
<td>40</td>
<td>274</td>
</tr>
<tr>
<td>56</td>
<td>384</td>
</tr>
<tr>
<td>64</td>
<td>512</td>
</tr>
<tr>
<td>80</td>
<td>768</td>
</tr>
<tr>
<td>96</td>
<td>1024</td>
</tr>
<tr>
<td>112</td>
<td>1792</td>
</tr>
<tr>
<td>120</td>
<td>2048</td>
</tr>
<tr>
<td>128</td>
<td>2304</td>
</tr>
</tbody>
</table>

RSA 512–2048 bits
DSS 512–1024 bits
Digital Signatures

One-way function. Easy to produce hash from message, “impossible” to produce message from hash

Hash of Message
s74hr7sh7040236fw

Sign Hash with Private Key
Signature = “Encrypted”
Hash of Message

Signature Verification

Decrypt the Received Signature
Decrypt Using Alice’s Public Key
Hash of Message
If Hashes Are Equal, Signature is Authentic

Message with Appended Signature
Re-Hash the Received Message
Hash Function
Hash Message
Digital Envelope

Alice Encrypts Message with a Random Secret Key

Encrypt the Secret Key with Bob’s Public Key

Bob Decrypts the Secret Key with His Private Key, then Decrypts the Message

Used During CA Transactions

Enrolling a Device with a CA

• Generate public/private keys
• Retrieve certificate from CA
• Send certificate request to CA
• CA signs certificate
PKI Deployment

CA Relationships—Hierarchy and Cross-Certification

Certificate Authority
Certificate User
Certificate (Points Issuer to Subject)
Cross Certificate

Alice → Bob → Carol
Subject Names

- subjectDN
  DN—X.500 distinguished name

- subjectAltName
  DNS name, email address, URIs, IP address

A PKC must have at least one

Encoding of Certificates

- Format of certificate is ASN.1
- DER (Distinguished Encoding Rules) produces octets for transmission
  E.g. Tag length value
  02 01 7F = integer 127
- Base 64 converts octets to ASCII for display (write t)
Distribution of CRLs

- Rate may vary according to security of the transaction
- Must be scheduled regardless of change in status
- Polling
  
  Client polls according to advertised interval
  CA or directory server can be polled
  Black hole between revocation and next scheduled update

Distribution of CRLs

- Push
  
  Broadcast
  Reliable transport
  Bandwidth Intensive
  Who needs them?

- On-line status checking
  
  Client initiated
  On-line query
  Info available 24 x 7
Reasons for Revocation

- Compromise of subject’s private key
- Change in subject name
- Change of subject’s affiliation
- Violation of CAs policies
- Compromise of CAs private key

Revoked
Cert 12345
Cert 12241
Cert 22333

PKI Deployment Guidelines

- Start with the root, move it off-line?
- Implement subordinate CAs
- Implement RAs
- Create CRL and certificate repository
- Define CRL update period
PKI Deployment Guidelines

- Define network connectivity
- Facilitate enterprise re-organization
- Administrative delegation
- Service availability

PKI Deployment

CA Database Capacity

<table>
<thead>
<tr>
<th>Service Size</th>
<th>Minimum Physical Memory</th>
<th>Recommended Physical Memory</th>
<th>Expected Database Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>Up to 10 KB Certificates</td>
<td>64 MB</td>
<td>128 MB</td>
<td>200 KB</td>
</tr>
<tr>
<td>10 KB–100 KB Certificates</td>
<td>128 MB</td>
<td>256 MB</td>
<td>200 KB–2 GB</td>
</tr>
<tr>
<td>100 KB–1 MB Certificates</td>
<td>256 MB</td>
<td>512 MB</td>
<td>2 GB–20 GB</td>
</tr>
</tbody>
</table>
Causes of PKI Failure

• Compromise of a private key
• Physical security problems
• Trustworthiness of administrators
• Security level of the CA
• Reliability of the CA
• Compromise of trust model

Simple Certificate Enrollment Protocol

• PKCS #7 for signing and enveloping
• PKCS #10 for certificate request
• HTTP and LDAP for transport
• Requires manual authentication during enrollment
• CRL distribution is manual
SCEP Overview—Distribution of CA/RA Certificates

Get CA/RA Cert: HTTP Request Message

Send CA/RA Cert: HTTP Response Message

Compute Fingerprint and Call CA Operator

Operator Check Fingerprint

SCEP Overview—Certificate Enrollment

PKCSReq: PKI Cert. Enrollment Message

CertRep: pkistatus = PENDING

Operator Check Fingerprints

Compute Fingerprint and Call CA Operator

CertCertInitial: Polling Message

CertRep: pkistatus = GRANTED Certificate Attached
SCEP Overview—CRL Distribution

GetCRL: PKI CRL Query Message

CertRep: CRL Attached

Cache the CRL

SCEP Overview—Certificate Access

GetCert: PKI Cert Query Message

CertRep: pkiStatus = GRANTED
Certificate Attached

Receive the Certificate
Validating a Certificate

- The recipient of the signed data verifies that the identity of the sender matches the identity contained in the PKC.
- Validate that no PKC in the chain is revoked via the retrieval of a current CRL.

Validating a Certificate

- The recipient verifies that the data does not contain values for which the PKC indicates signer is not authorized for.
- Verify that the data was not altered since signing by using the public key in the PKC.
Validating the Certificate Debug

**ISAKMP (0:1):** Checking ISAKMP transform 3 against priority 4 policy
**ISAKMP:** encryption DES-CBC
**ISAKMP:** hash SHA
**ISAKMP:** default group 1
**ISAKMP:** auth RSA sig
**ISAKMP:** life type in seconds
**ISAKMP:** life duration (VPI) of 0x0 0x0 0x70 0x80
**ISAKMP (0:1):** atts are acceptable. Next payload is 3
**ISAKMP (0:1):** processing vendor id payload
**ISAKMP (0:1):** SA is doing RSA signature authentication
**ISAKMP (1):** SA is doing RSA signature authentication using id type ID_FQDN

**ISAKMP:** Main Mode packet contents (flags 1, len 1676):
- ID payload
- CERT payload
- SIG payload
- CERT-REQ payload
**ISAKMP (0:1):** processing ID payload. message ID = 0
**ISAKMP (0:1):** processing CERT payload. message ID = 0
**ISAKMP (0:1):** processing a CT_X509_SIGNATURE cert
**ISAKMP (0:1):** cert approved with warning
**ISAKMP (0:1):** processing SIG payload. message ID = 0
**ISAKMP (1):** processing CERT_REQ payload. message ID = 0
**ISAKMP (1):** peer wants a CT_X509_SIGNATURE cert
**ISAKMP (1):** peer want cert issued by CN = munchkinca, OU = Punknet, O = Cisco Systems, L = Seattle, ST = WA, C = US, EA =<16>
ntimms@cisco.com
Using a CA—
Entrust Configuration

- ip domain-name cisco.com
- crypto isakmp policy 4
- crypto ca identity cisco.com
  
enrollment mode ra
  
enrollment url http://10.0.0.2/cgi-bin
  
query url ldap://10.0.0.2
  
crl optional

CA and SCEP Example

Step 1—Generate Public/Private Keys

barney(config)#crypto key gen rsa usage

The name for the keys will be: barney.cisco.com

Choose the size of the key modulus in the range of 360 to 2048 for your
Signature Keys. Choosing a key modulus greater than 512 may take
a few minutes.

How many bits in the modulus [512]:

Generating RSA keys ...

[OK]

Choose the size of the key modulus in the range of 360 to 2048 for your
Encryption Keys. Choosing a key modulus greater than 512 may take
a few minutes.

How many bits in the modulus [512]:

Generating RSA keys ...

[OK]
CA and SCEP Example

Step 1—Generate Public/Private Keys

barney#sho crypto key mypublic rsa
% Key pair was generated at: 01:18:43 UTC Mar 1 1999
Key name: barney.cisco.com
Usage: Signature Key
Key Data:
305C300D 06092A86 4886F70D 01010105 00004B00 30480241 00BEDC6C FBD2721F 2AF7521 F2DE3D04 D3229759 7908C8F1 64F0E68F 0116CF6A 897D2120 2D4BFC80
% Key pair was generated at: 01:18:45 UTC Mar 1 1993
Key name: barney.cisco.com
Usage: Encryption Key
Key Data:
305C300D 06092A86 4886F70D 01010105 00004B00 30480241 00C06DC2 3AE2BF72 CE9FD6F6 55C13A0D A3C183D5 1E7E4523 E8863DCC D852FD32 86461BBC F10EEA77
8A6A5AC9 AFEF6B0A 03107565 03384DB4 4E6C4A77 0C594B10 31020301 0001

Step 2—Request the CA and RA Certificates
Manually verify Fingerprint of CA

barney(config)#cryp ca auth cisco.com
Certificate has the following attributes:
Fingerprint: 1A5416D6 2EEE8943 D11CCE1 3DEE9CE7
% Do you accept this certificate? [yes/no]: y
CA and SCEP Example

Step 2—Request the CA and RA Certificates
Manually Verify Fingerprint of CA

Step 3—Enroll the Router with the CA

barney(config)#cry ca enrol cisco.com
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this password to the CA Administrator in order to revoke your certificate. For security reasons your password will not be saved in the configuration. Please make a note of it.

Password:
Re-enter password:

% The subject name in the certificate will be: barney.cisco.com
% Include the router serial number in the subject name? [yes/no]: n
% Include an IP address in the subject name? [yes/no]: n
Request certificate from CA? [yes/no]: y
Step 3—Enroll the Router with the CA
Fingerprints sent to CA for manual verification

barney(config)#
   Signing Certificate Request Fingerprint:
   4C6DB57D 7CAF8531 7778DBB3 CCEB1FFB
   Encryption Certificate Request Fingerprint:
   D33447FE 71FF2F24 DA98EC73 822BE4F7
Step 4—CA grants Certificates
Status Pending -> Available

barney# sho cryp ca cert
Certificate
Subject Name
Name: barney.cisco.com
Status: Pending
Key Usage: Signature
Fingerprint: 4C6DB57D 7CAF8531 7778DDB3 CCEB1FFB

Certificate
Subject Name
Name: barney.cisco.com
Status: Pending
Key Usage: Encryption
Fingerprint: D33447FE 71FF2F24 DA98EC73 822BE4F7

Step 4—CA Grants Certificates
PKIX and the IETF

- Handles interoperability issues
- Profiles for X.509 v3 certificates to be used by security protocols like IPSec, new extensions
- Operational protocols for certificate and CRL distribution, e.g. LDAP, HTTP, FTP
- Management protocols for the support of interactions between a CA and client system, i.e. register, revoke via standard messages and exchange protocols (CRMF, CMMF, CMP, CMC)
- Policy outline via certificate policy (CP) and certification practice statement (CPS)

Deploying IPSec in the Enterprise
Agenda

- VPN Deployment Examples
  - Hub and Spoke
  - Hub and Spoke with Redundancy
  - Very Large Networks and Multihop Crypto
  - Remote Access Support for Clients and Gateways
  - Full Mesh Networks
  - Tunnel Endpoint Discovery (TED)
- Guidelines for Migration to Crypto in Large Networks
- GRE Configuration for Routing Support

Example 1—Hub and Spoke Topology

Remote1
192.168.100.0

172.21.115.0

HQ1
172.21.114.0

Remote2
192.168.150.0

172.21.116.0

IPSec
Example 1—Central Site Router

Config 1

crypto map HQ 10 IPSec-isakmp
set peer 172.21.115.1
set peer 172.21.116.1
set transform-set encrypt-des
match address 101

With one all inclusive ACL list, first peer in the crypto map is tried regardless of whether it is the correct one. If it is not, the initiator waits 45 seconds, (3 x 15 seconds for each retry for Main Mode IKE), before trying the next peer on the list.

Example 1—Central Site Router

Config 2

crypto map HQ 10 IPSec-isakmp
set peer 172.21.115.1
set transform-set encrypt-des
match address 101
crypto map HQ 20 IPSec-isakmp
set peer 172.21.116.1
set transform-set encrypt-des
match address 102

A separate crypto map instance and a unique ACL is used for each possible remote site ensuring that the correct peer is contacted first.
Example 2—Hub and Spoke with Redundancy

Example 2—Hub and Spoke with Redundancy Config

crypto map remote1 10 IPSec-isakmp
set peer 172.23.114.1
set peer 172.23.114.2
set transform-set encrypt-des
match address 101
access-list 101 permit ip 192.168.100.0 0.0.0.255 <hq-subnets>

This crypto map is assigned to both primary and backup subinterfaces on each remote. The dual set peer statements will provide redundancy at the HQ site. Keepalives will facilitate SA re-establishment with new peer.
Example 3—Large Networks and Multihop Crypto

- Allows the distribution of load across multiple central site routers, capacity issues
- If any site can communicate with any other, configs can get long and confusing
- Requires distinct subnets and crypto maps per interface on the central site routers
router A
crypto map spoke 1 ipsec-isakmp
set peer B

router A
crypto map spoke 2 ipsec-isakmp
set peer X

router HQ
requires nothing specific for spoke to spoke crypto as it will simply route the IPSec packets between the spokes.

For hub to spoke crypto, the statements will look like those on router A….one for each site

router HQ

For hub to spoke crypto, one crypto map for each site including additional ACLs for spoke to spoke subnets apply to each interface

crypto map spokeA 1 ipsec-isakmp
set peer A
match HQ to 192.168.100.0
match 192.168.150.0 to 192.168.100.0

router B
crypto map spoke 1 ipsec-isakmp
set peer HQ

router B
crypto map spoke 1 ipsec-isakmp
set peer HQ
Spoke to Spoke IPSec
Point to Multipoint

192.168.100.0
172.21.115.0

192.168.150.0
HQ

router A
crypto map spoke 1 ipsec-isakmp
set peer HQ

router B
crypto map spoke 1 ipsec-isakmp
set peer HQ

Problems here as A-HQ traffic creates a “map”
between A and HQ for 192.168.100.0 to
192.168.150.0, when HQ-B “map” created:
IPSEC(validate_transform_proposal) peer
address B not found

crypto map spoke 1 ipsec-isakmp
set peer A
match HQ to 192.168.100.0
match 192.168.150.0 to 192.168.100.0
crypto map spoke 2 ipsec-isakmp
set peer B
match HQ to 192.168.150.0
match 192.168.100.0 to 192.168.150.0

crypto dynamic-map AcceptRemote 20
set transform-set encrypt-des
crypto map dynamicHQ 10 IPSec-isakmp
dynamic AcceptRemote

A dynamic crypto map can simplify support for multiple
remotes. The caveat is that the central site router can
ever initiate the Sas. There is also a security problem if
dynamic crypto maps and used with wildcard pre-shared
keys—the initiators ID cannot be verified.
Example 4—Support for Remote Sites
Central Site Router Config 2

```
crypto dynamic-map AcceptRemote 20
  set transform-set encrypt-des
  crypto map dynamicHQ 10 IPSec-isakmp
    set peer x.x.x.x
    set transform-set encrypt-des
    match address 101
  crypto map dynamicHQ 20 IPSec-isakmp dynamic
    AcceptRemote
```

A crypto map can support both a static and dynamic definition. The dynamic is the catch-all. It is recommended that digital certificates are used for dynamic crypto maps when the remote is not at least capable of X-auth.

Example 5—Support for Remote Clients and Routers
Central Site Router Config 1

```
crypto dynamic-map client 20
  set transform-set encrypt-des
  crypto map mode client configuration address initiate
  crypto map mode client configuration address respond
  crypto map client 10 ipsec-isakmp dynamic client
```

The initiator may be a client, capable of mode config, or a router or client that does not support mode config. If the crypto map is configured for respond only, mode config will not be attempted by this gateway unless the remote requests it. If this router is set to initiate, it will be up to the remote to ignore mode config parameters if they are not supported.

**X-auth**
Example 6—Full Mesh Networks

• Multihop encryption?
• Tunnel endpoint discovery?

Tunnel Endpoint Discovery

How Do You Scale Large Intranets?
How TED Works

Tunnel Endpoint Discovery
- Provides automated peer discovery, easing scalability and configuration
- Provides improved availability by automating failover

TED Debug

13:11:35: IPSEC (tunnel discover request):
(key eng. msg.) src=10.0.0.130, dest=172.17.11.10,
src_proxy=10.0.0.0/255.255.255.0/0/0 (type=4),
dest_proxy=192.168.1.2/255.255.255.0/0/0 (type=1),
protocol=ESP, transform=esp-des esp-md5-hmac,
lifetime=120s and 4608000kb,
spt=0x0, conn_id=0, keysize=0, flags=0x4044
13:11:35: GOT A PEER DISCOVERY MESSAGE FROM THE SA MANAGER!!!
src=10.0.0.130
13:11:35: GOING TO 172.17.11.10, protocol 3, transform 2, hmac 1
13:11:35: ID of source is 10.0.0.0/255.255.255.0 and my address (not used now) is 192.168.1.2
13:11:35: ID of source is 192.168.1.2
13:11:35: ISAKMP (216): beginning peer discovery exchange
13:11:35: ISAKMP (216): sending packet to 172.17.11.10 (I) PEER_DISCOVERY
13:11:35: ISAKMP (216): received packet from 172.17.11.10 (I)
13:11:35: PEER_DISCOVERY
13:11:35: ISAKMP (216): processing vendor id payload
13:11:35: ISAKMP (216): processing payload. message ID = 0
13:11:35: ISAKMP (216): processing payload. message ID = 463659126
13:11:35: ISAKMP (216): received response to my peer discovery
probe ISAKMP: initiating IKE to 192.168.0.200 in response to probe.
Configuring TED

*crypto dynamic-map probe 1*
*Set transform desmd5*
*Match address 123*

*crypto map ted 1 ipsec-isakmp dynamic probe discover*

*Access-list 123 permit ip 10.0.0.0 0.0.0.255 172.17.11.0 0.0.0.255*

TED Caveats

- Needs unique subnets
- If using TED across the Internet, subnets must be public (registered) addresses
- Don’t go ahead without consulting your Cisco Engineer
Adding Crypto to Large Networks

- Like cutting over to a new routing protocol
  - AS boundary router to AS boundary router—InterAS IPSec
  - AS by AS—IntraAS crypto
- Multihop model
- Across AS—must be balanced
Configuring GRE Tunnels
Used for Multicast and Broadcast Support

• crypto map
  my_crypto_map 10
  set algorithm esp-des
  set peer 2.2.5.2
  match address 128

• router (protocol)
  passive interface S0

• interface Tunnel0
  ip unnumbered S0
  tunnel source S0
  tunnel destination 2.2.5.2
  crypto map my_crypto_map

• interface Serial0
  ip address 2.2.5.3 255.255.255.0
  crypto map my_crypto_map

• access-list 128 permit gre host
  2.2.6.3 host 2.2.5.2

Multiservice and IPSec
Agenda

- Voice and IPSec
  - Factors to Consider for Voice
  - Voice and IPSec Example
  - Summary, Statistics, and Conclusions
  - Notes and Caveats
- Voice and IPSec with QoS
  - QoS Features Summary
  - Problems QoS and IPSec
  - Voice, QoS, and IPSec Example
  - Summary, Statistics, and Conclusions
  - Notes and Caveats

Factors to Consider for Voice

Factors to Consider for Voice:

1. Serialization Delay
2. Network Transit Delay
3. Processing Delay
4. Propagation Delay

First Bit Transmitted

Last Bit Received

Network Time
Factors to Consider for Voice

- **Delay**
  - Processing—PCM to G.729 to packet
  - Serialization—time it takes to get a packet out of the router, each “hop” generally has a fixed delay
  - Propagation—end-to-end
  - Variable—other factors, such as IPSec will add this. Too much variable delay introduces jitter which is detrimental to voice quality

- **Packet size and mix**
  - A VoIP packet is around 38 bytes over frame, and 64 bytes across Ethernet
  - IPSec will add its headers and may push the packet size to > 100 bytes
  - At 50 pps 100 byteframes, a 56 kb link can only accommodate a single call (50 x 100 bytes = 40 kb)
  - RTP header compression is not available to IPSec frames
  - Without QoS, all packets are treated equally by IPSec
VoIP and IPSec Scenario

VoIP and IPSec Config Notes

- The topology was implemented using two different serial link speeds
  - 2 MB
  - 128 KB
- The VoIP/IPSec routers were 1750s
- The effect of IPSec using both software, and hardware was tested
- Only one voice call was made
VoIP and IPSec Configs

hostname router4
!
memory-size iomem 25
ip subnet-zero
!
crypto isakmp policy 1
  encr 3des
  authentication pre-share
  group 2
  crypto isakmp key cisco address 10.0.1.1
  !
crypto ipsec transform-set 3dessha esp-3des esp-sha-hmac
  !
crypto map voip local-address Loopback0
crypto map voip 1 ipsec-isakmp
  set peer 10.0.1.1
  set transform-set 3dessha
  match address 101
!
interface Loopback0
  ip address 172.17.12.1 255.255.255.0
!
interface Serial0
  ip address 192.168.2.2 255.255.255.0
  !
  interface FastEthernet0
  ip address 172.17.11.1 255.255.255.0
  !
  ip route 0.0.0.0 0.0.0.0 192.168.2.1
  !
  access-list 101 permit ip 192.168.2.0 0.0.0.255
  192.168.1.0 0.0.0.255
  !
  voice-port 2/0
  !
  voice-port 2/1
!
dial-peer voice 111 voip
destination-pattern 111
session target ipv4:10.0.2.1
!
dial-peer voice 444 pots
destination-pattern 444
port 2/0

hostname router1
!
crypto isakmp policy 1
  encr 3des
  authentication pre-share
  group 2
  crypto isakmp key cisco address 192.168.2.2
  !
crypto ipsec transform-set 3dessha esp-3des esp-sha-hmac
  !
crypto map voip local-address Loopback0
crypto map voip 1 ipsec-isakmp
  set peer 172.17.12.1
  set transform-set 3dessha
  match address 101
!
interface Loopback0
  ip address 10.0.1.1 255.255.255.0
!
interface Serial0
  ip address 192.168.1.2 255.255.255.0
  !
  interface FastEthernet0
  ip address 10.0.0.20 255.255.255.0
  !
  ip route 0.0.0.0 0.0.0.0 192.168.1.1
  !
  access-list 101 permit ip 192.168.1.0 0.0.0.255
  192.168.2.0 0.0.0.255
  !
  voice-port 2/0
  !
  voice-port 2/1
!
dial-peer voice 111 voip
destination-pattern 111
session target ipv4:172.17.12.1
!
dial-peer voice 444 voip
destination-pattern 444
session target ipv4:172.17.12.1
**VoIP and IPSec**

<table>
<thead>
<tr>
<th>Description</th>
<th>Speed</th>
<th>RT Delay</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clear Voice Only</td>
<td>2 MB</td>
<td>7 ms</td>
</tr>
<tr>
<td>Clear Voice Only</td>
<td>128 KB</td>
<td>69 ms</td>
</tr>
<tr>
<td>IPSec 3DES, SHA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Voice Only (SW)</td>
<td>2 MB</td>
<td>22 ms</td>
</tr>
<tr>
<td>IPSec 3DES, SHA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Voice Only (SW)</td>
<td>128 KB</td>
<td>104 ms</td>
</tr>
<tr>
<td>IPSec 3DES, SHA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Voice Only</td>
<td>2 MB</td>
<td>11–12 ms</td>
</tr>
<tr>
<td>IPSec 3DES, SHA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Voice Only</td>
<td>128 KB</td>
<td>95 ms</td>
</tr>
</tbody>
</table>

**VoIP and IPSec Conclusions**

- Jitter was experienced during a re-key when PFS was configured
- No significant packet loss even with software crypto, although there was only the *one* call
- Without QOS, the effect of combining voice and data traffic with IPSec makes the solution infeasible
- No significant impact to call setup time, although during heavy usage this will be a problem, e.g. setting up multiple IKE SAs simultaneously
- More tests are required to determine the effect on voice quality of a system under load
VoIP and IPSec Notes

- **IPSec ACL must specify WAN endpoints/subnets to facilitate RTP, H.225**
- **Port numbers used for VoIP may not be well-known and may be negotiated**

Cisco IOS® QoS Features

<table>
<thead>
<tr>
<th>Service Provided</th>
<th>Mechanism</th>
<th>Network Effect</th>
</tr>
</thead>
<tbody>
<tr>
<td>Congestion Avoidance</td>
<td>RED, WRED, Flow RED</td>
<td>• Avoid Congestion by Notifying Source</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Prioritize which Traffic is Told to Reduce</td>
</tr>
<tr>
<td>Congestion Management</td>
<td>PQ, CQ, WFQ, CB WFR, MDRR</td>
<td>• Bandwidth Management: Traffic Priority</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Set Servicing Sequence</td>
</tr>
<tr>
<td>Classification</td>
<td>CAR, Policy Routing, DSCP, NFCII</td>
<td>• Sets IP Precedence/DSCP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• By Application, Protocol, Address, etc</td>
</tr>
<tr>
<td>Metering (Policing)</td>
<td>CAR</td>
<td>• Enforce a Maximum Transmission Rate</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Conform or Exceed Thresholds</td>
</tr>
<tr>
<td>Shaping</td>
<td>GTS, FRTS</td>
<td>• Conforms Traffic to Committed Bandwidth</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Interwork with Layer 2 Notification e.g., BECN</td>
</tr>
<tr>
<td>Compress</td>
<td>CRTP</td>
<td>• Reduce the Volume of Traffic Sent</td>
</tr>
<tr>
<td>Fragment</td>
<td>LFI, FRF.12</td>
<td>• Reduce Delay on Slower Speed Links</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Split, Recombine Larger Frames</td>
</tr>
</tbody>
</table>
Problems with IPSec and QoS

- A problem is that IPSec uses FIFO, all packets are treated the same.
- Then after encryption, it is not possible for other QoS mechanisms like WFQ to determine the contents of the packets.

Problems with IPSec and QoS

- Even if VoIP can set IP precedence before handing packets to IPSec (e.g. `ip precedence 7`), nothing is gained. IPSec will copy the TOS bits to the outer header. After IPSec, QoS may help get higher priority traffic out of the router quicker, but the added delay caused by the crypto has already been introduced.
Problems with IPSec and QoS

- What is required is a QoS mechanism that can honor or set IP precedence before IPSec. This requires the QoS occurs inbound to the IPSec router, which means the VoIP must be done on a separate router.

A Possible Solution—Committed Access Rate (CAR)

- A method for QoS prior to IPSec
- Two functions
  - Packet classification—IP precedence and QoS group setting
  - Access bandwidth management through rate limiting (policing)
VoIP, QoS and IPSec Scenario

VoIP, QoS, and IPSec Config Notes

- IPSec continued to be performed by the 1750 routers in hardware
- Router5 and router6 were 2600s
- Only one voice call and one data stream were used
- The two serial link speeds were again used
- IP Precedence was set on the VoIP routers with CAR enabled inbound on the IPSec routers
- CAR parameters may not be realistic but were chosen to prove the point
VoIP, CAR, and IPSec Configs

**hostname router5**
voice-port 2/0
!
voice-port 2/1
!
dial-peer voice 111 voip
destination-pattern 111
session target ipv4:172.17.13.1
ip precedence 7
!
dial-peer voice 444 pots
destination-pattern 444
port 2/0

**hostname router1**
!
rate-limit input access-group 102 96000 100000
100000 conform-action transmit
exceed-action transmit
rate-limit input access-group 103 16000 20000
20000 conform-action transmit
exceed-action drop
speed auto
!
access-list 102 permit ip host 10.0.2.1 host 172.17.13.1 precede
access-list 103 permit ip any any

VoIP, QoS, and IPSec

<table>
<thead>
<tr>
<th>Description</th>
<th>Speed</th>
<th>RT Delay</th>
<th>Loss (Late)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clear Voice, Data, No QoS</td>
<td>2 MB</td>
<td>9 ms</td>
<td></td>
</tr>
<tr>
<td>Clear Voice, Data, No QoS</td>
<td>128 KB</td>
<td>115–300 ms</td>
<td>172</td>
</tr>
<tr>
<td>IPSec 3DES, SHA Voice, Data, No QoS</td>
<td>2 MB</td>
<td>14–30 ms</td>
<td></td>
</tr>
<tr>
<td>IPSec 3DES, SHA Voice, Data, No QoS</td>
<td>128 KB–2000</td>
<td>350–600 ms</td>
<td>&gt;500</td>
</tr>
<tr>
<td>IPSec 3DES, SHA Voice, Data, No QoS</td>
<td>128 KB–1500</td>
<td>~ 200 ms</td>
<td>~ 170</td>
</tr>
<tr>
<td>Clear Voice, Data, CAR</td>
<td>2 MB</td>
<td>7–11 ms</td>
<td></td>
</tr>
<tr>
<td>Clear Voice, Data, CAR</td>
<td>128 KB</td>
<td>67 ms</td>
<td></td>
</tr>
<tr>
<td>IPSec 3DES, SHA Voice, Data, CAR</td>
<td>2 MB</td>
<td>7–11 ms</td>
<td></td>
</tr>
<tr>
<td>IPSec 3DES, SHA Voice, Data, CAR</td>
<td>128 KB</td>
<td>69–70 ms</td>
<td>19</td>
</tr>
</tbody>
</table>
VoIP, QoS, and IPSec

Conclusions

- CAR can also be used to set precedence and manage traffic flow
- CAR is required to set precedence for traffic returning from the responded to the call
- More tests are required to determine the effect on voice quality of a system under load
QoS and IPSec Notes

- Diff-serv, NBAR, CAR—entire TOS byte is copied to the IPSec header so precedence can be applied. The additional length may change the packet’s service characteristics
- QoS must be implemented before IPSec to overcome the FIFO problem—pre-classification planned

Advanced Topics in Enterprise VPNs and PKI

Session 2403
Please Complete Your Evaluation Form
Session 2403