Extranet Architecture

Session 1405
Agenda

- What Is an Extranet?
- Why Use an Extranet?
- Types of Extranets
- Case Study
- Conclusions

What Is an Extranet?

- A semi-public intranet
- A semi-private Internet
- A private network that connects independent peer organizations
Why Use an Extranet?

- Business model (policy)
- Control
  - Security
  - Quality of Service
- Costs

Who Connects to Extranets?

- Suppliers
- Partners
- Customers
- Co-petitors
Types of Extranets

- Bilateral
- Overlay
- Shared
**Extranet—Bilateral**

- Private circuits to suppliers, partners, and customers
- Example: Cisco

---

**Extranets—Cisco Systems**

Partners/Extranet (1999)
Extranet—Bilateral

Bilateral—Physical Connection

- Single line to a partner
  - Leased line
  - Other transport service
- Usually not through the Internet
Bilateral—Addressing

- Registered IP addresses preferable
  - Address authority assigned
  - Globally unique
- Private addresses—RFC 1918
  - Requires coordination
  - Must be locally unique

Private Addressing (1)

- Private address to public address
- Could cause issues in the future
Private Addressing (2)

- Private address to private address
- Requires coordination to avoid conflicts

Private Addressing Issues

- Address conflict resolution options
  - Re-number systems --or--
  - Use Network Address Translation (NAT)
What Is NAT?

- Described in RFC 1631
- Technique of rewriting IP addresses in headers and application data streams according to a defined policy
- Does not work with all applications
- See also Networkers session:
  1306 Expanding ISP and Enterprise Connectivity with Cisco IOS™ NAT

Address Translation Example

<table>
<thead>
<tr>
<th>SA = Source Address</th>
<th>Outside Local IP Address</th>
<th>Outside Global IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.0.2</td>
<td>131.108.1.1</td>
<td>10.0.0.20</td>
</tr>
<tr>
<td>10.0.0.3</td>
<td>131.108.1.2</td>
<td>10.0.0.21</td>
</tr>
</tbody>
</table>
Bilateral—Routing

- Choose the right routing method
  Two administrative domains
  Need reachability information

Routing Choices

- Static Routes
- Exterior Gateway Protocols
- Interior Gateway Protocols
- See also Networkers session:
  301 Introduction to Routing
Static Routes

• Routes configured manually
  High control of routing information
• No bandwidth used for routing updates
• Recommended method

Exterior Gateway Protocols

• Border Gateway Protocol—BGP
  Simple to configure reachability
  Designed for multiple administrative domains
• See also Networkers sessions:

  309 Deploying BGP
  317 Advanced BGP and Troubleshooting
Interior Gateway Protocols

• Creates additional administrative domain
• Generally not recommended

Interior Gateway Protocols

• See also Networkers sessions:
  307 Deploying EIGRP/IGRP
  308 Deploying OSPF/NLSP/IS-IS
  315 Advanced IP EIGRP and Troubleshooting
  316 Advanced OSPF/NLSP/IS-IS and Troubleshooting
Bilateral—Security

• Filters
• Firewall

Controlling Traffic

Partner #1

Corporate Intranet

Partner #2
Security—Route Filtering

```
201.222.5.0

ip route 201.222.5.0 255.255.255.0 serial 0
! create static route
router eigrp 1
network 131.108.1.0
default-metric 10000 100 255 1 1500
redistribute static
distribute-list 3 in serial 0
! do not accept any other routing information
access-list 3 deny
passive-interface serial 0
```

Security—Traffic Filtering

```
201.222.5.0

ip access-list standard them2us
permit 201.222.5.0 0.0.0.255 131.108.1.12 0.0.0.0
deny any
ip access-list standard us2them
permit 131.108.1.0 0.0.0.255 201.222.5.5 0.0.0.0
deny any
! only allow traffic between specific systems
interface serial 0
ip access-group them2us in
ip access-group us2them out
```
Avoid Transit Situations

Security—Firewalls

• What is a firewall?
• See also Networkers sessions:
  302 Introduction to Information Security
  311 Deploying Security Technology
  318 Advanced Security Technology Concepts
  1303 Update on Firewall Technologies
What Is a Firewall?

“All traffic from inside to outside and vice-versa must pass through the firewall

Only authorized traffic, as defined by the local security policy, will be allowed in

The firewall itself is immune to penetration”

Bellovin and Cheswick “Firewalls and Internet Security, Repelling the Wily Hacker”

Firewall Features

• Filtering: static, dynamic, content, state
• Application recognition/inspection
• Attack detection/prevention
• AAA
• Management, logging
What Is a “Security Policy?”

“A security policy is a formal statement of the rules by which people who are given access to an organization’s technology and information assets must abide.

Source: RFC 2196,
Site Security Handbook draft
Security Questions

- Who can see what information?
- Who can change it?
- From where?
- How protected is it?
- What are the assets?
- What is the cost?

Security Policy Objective

- Balance Business Needs with Risks

**Transparent Access**
- Connectivity
- Performance
- Ease of Use
- Manageability
- Availability

**Security**
- Authentication
- Authorization
- Accounting
- Assurance
- Confidentiality
- Data Integrity

Policy Management
Bilateral—Management

- Control
  Boundary of administrative domain
- Back up

Network Management

- See other Networkers sessions:
  801 Evolution of Network Management Technologies
  802 Policy and Management Technologies and Protocols
  803 Network Management within Campus Networks
  804 Establishing Best Practices for Network Management
Back Up Connections

- Dial-up access—Telephone service, ISDN
- Usually secondary connection only used in case of primary connection failure

Bilateral Extranets

- Pros
  - Good for small numbers of connections
  - High degree of control
- Cons
  - Requires much configuration and coordination
  - Management of physical equipment
Extranets—Overlay

- Similar to Bilateral
  Uses tunneling technology
- Virtual Private Networks (VPN)
- Allows new or different protocols
- Example: IPv6 Backbone
Extranets—IPv6—6Bone

UK IPv6 Resource Centre
Lancaster University Computing Department
Backbone Site Connectivity for 6Bone

Lancs 6iNet

Tue. May 11 09:30:02 1999

STATIC
RIPng
IDRPv6
BGP4+
UNKNOWN

Extranets—Overlay

Internet

Corporate Intranet

ISP A
ISP B
ISP C
ISP E

Peer #1
Peer #2
Peer #3
Choosing a Service Provider

- Do they offer the service you need?
- Do they offer the service in the locations you require?
- Do they offer the service at a fair price?
Overlay: Addressing

- Registered address required to connect to Internet
  - Your assigned address space
  - Service provider address space
- Must be unique
- NAT for private addressing

Overlay: Routing

- Establish routing to the Internet
- Build tunnels
- Establish routing “virtual” bilateral links
Routing to the Internet

- Normal Internet connectivity
- Static or BGP as specified by you and your service provider

Tunnels

- Provide a point-to-point connection between two routers via a virtual software interface
- See also Networkers sessions:
  305 *Introduction to VPNs and Tunneling Technology*
  313 *Deploying VPNs and Tunneling Technology*
Layer 2 Tunnel Protocols

- **PPTP** (Point-to-Point Tunneling protocol) Microsoft/Ascend/3COM Proprietary
- **L2F** (Layer 2 Forwarding) Cisco Proprietary (in Cisco IOS™ 11.2+)
- **L2TP** (Layer 2 Tunneling Protocol) IETF Draft combining the best of PPTP and L2F; Industry standard track

Generic Routing Encapsulation—GRE

- RFC 1701, 1702
- Customer-independent address space and routing information
- Encapsulates multiprotocol packets in tunnels
- Mesh of virtual point-to-point interfaces
**IPSec**

- RFC 1825–1829
- Standards define negotiation, protocols, and formats
- Network layer encryption and authentication

**Multi Protocol Label Switching—MPLS**

- Emerging IETF industry standard based on Cisco’s MPLS submission
- Forwards packets based on labels
- No address translation needed
Encryption and Decryption

Clear-Text

Our next acquisition is...

Cipher Text

Encryption

Decryption

Our next acquisition is...

Lksdjf98pj diluted;":",& oidgu90e

Encryption Alternatives

Application-Layer Encryption

Transport/Network Layers (3-4)

Network-Layer Encryption

Link/Physical Layers (1-2)

Link-Layer Encryption
Virtual Private Networks

• More Networkers sessions:
  1113 New Developments for the Enterprise Virtual Private Network
  1206 Deploying Enhanced Services

“Virtual” Bilateral Links

• Point to point tunnels
• Static routes preferred
• Firewall placement is important
• Based on security policy

Establishing Security

• Know where and how to deploy security technologies to maximize your coverage.
Multiple Security Policies

- Overlay extranets add complexity to security policies

Network Security

- See also Networkers sessions:
  - 1112 Introduction to Cisco Security Manager
  - 1305 Intrusion Detection and Scanning with Active Audit
  - 1308 Cisco Security Consulting Services Update
Overlay: Management

• Control

Administrative domain begins at Service Provider demarcation

• Back up

Quality of Service

• Service agreements only pertain to Internet connection

• No control over “cloud”
• Many Service Providers offer VPN or Extranet services
• Commitment to Service Level and QoS

Service Level Agreement

Acme ISP’s VPN Service Level Agreement
December 1998 Corporation

<table>
<thead>
<tr>
<th>Service</th>
<th>Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overall Network Availability</td>
<td>99.7%</td>
</tr>
<tr>
<td>Dial Port Availability</td>
<td>99.5%</td>
</tr>
<tr>
<td>End-to-End Latency</td>
<td>&lt;= 150 ms Roundtrip</td>
</tr>
<tr>
<td>Local Loop Availability</td>
<td>99.7%</td>
</tr>
<tr>
<td>Packet Loss</td>
<td>&lt;1%</td>
</tr>
<tr>
<td>Firewall Updates</td>
<td>Within 24 Hrs. after Cert. Alert</td>
</tr>
</tbody>
</table>

Acme ISP promises that if it abrogates any of these committed service levels, it owes Big International Corporation a refund of one full month’s charges.

Signed:

Source: Forrester Research
**Back-up: Multiple Internet Connections**

- Routing is static through the tunnel
- The tunnel itself can be dynamic

**Overlay Extranets**

**Pros**
- Takes advantage of installed Internet connection
- (Usually) No new hardware, software configuration only

**Cons**
- No control over data routing
- No control over quality of service
- Security concerns
Overlay Extranets—Managed Service

• Pros
  Service Level Agreements
  Quality of Service
  Network management

• Cons
  Limited to service offering
  Perceived security issues
Extranet—Shared

• Internet model
  Major player(s) act as service providers
  Contracted service provider
  Create organization to be service provider

• Organized around “Community of Interest”

• Examples: Internet2 (I2), ANX

Extranets: Internet 2
Shared—Physical Connection

- Connection usually specified by Shared Network Provider

Shared—Addressing

- Must be unique within shared network
  
  Your assigned address space
  
  Shared network address space

- NAT for private addressing
**Shared—Routing**

- Similar to Internet connectivity
- Static or BGP as specified by the Shared Network Provider

**Shared—Security**

- Security policy specified by Shared Network Provider
- Usually with input from “Community of Interest”
**Security Policy**

- You have control over your connection
- Similar to Internet security policy
- Perceived “safer” due to limited membership

**Shared: Management**

- Control
  Administrative domain begins at Shared Network demarcation
  Back up
Shared Extranet

• Pros
  Clear responsibility for transport and connectivity
  Enforcement of consistent policy
  Potentially infinitely scalable

• Cons
  Legal and Political sensitivity
  Commonly a limited use policy enforced

Case Study
Case Study—Printing Service

- Store front in shopping area
- Customers walk in or ship print jobs

- Company connects to the Internet
  - Electronic mail
  - Public web site
Case Study—Printing Service

• Start with email attachments, but too large and awkward
• Add secure “drop off” system for customers to leave print jobs

Case Study—Printing Service

• Create extranet by adding bilateral connection to graphics partner
Case Study—Printing Service

- Back up connection by building encrypted tunnel through the Internet

Case Study—Printing Service

- Add publishing partner to extranet
Case Study—Printing Service

- Outsource network to service provider

Case Study—Printing Service

- Create shared network linking printers, publishers, authors, book stores
Conclusions

Types of Extranets

- Bilateral
- Overlay
- Shared
Extranet Addressing

• Unique addresses required
  Address authority assigned
  Service provider assigned
• Address translation can be used to handle private addresses

Extranet Routing

• Key is reachability
  Between you and partner/peer
  Between you and service provider
• Control of routing information
  Static routes or BGP recommended
  Filtering of routing information
  Filtering of traffic
### Extranet Security

- Intranets focus on **us** and **them**
- Extranets are more like this:

---

### Extranet Management

<table>
<thead>
<tr>
<th>Pro</th>
<th>Extranet Service/Shared</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bilateral/Overlay</td>
<td>Pro</td>
</tr>
<tr>
<td>Secure</td>
<td>Globally available</td>
</tr>
<tr>
<td>Controlled</td>
<td>Redundant</td>
</tr>
<tr>
<td>Self destined</td>
<td>Less expensive</td>
</tr>
<tr>
<td>Self managed</td>
<td>Greater connectivity</td>
</tr>
<tr>
<td></td>
<td>Simplified WAN</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Con</th>
<th>Extranet Service/Shared</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bilateral/Overlay</td>
<td>Con</td>
</tr>
<tr>
<td>No economies of scale</td>
<td>Third party</td>
</tr>
<tr>
<td>Local skill required</td>
<td>Perceived less secure</td>
</tr>
<tr>
<td>Investment in technology</td>
<td></td>
</tr>
</tbody>
</table>

---

**PRO** • Secure • Controlled • Self destined • Self managed

**CON** • No economies of scale • Local skill required • Investment in technology

---

---
Extranet Conclusion

• A mix of each is most likely
• Connect to partners, suppliers, customers in the best way that supports your specific business model

Thank You
Please Complete Your Evaluation Form

Session 1405