Hardware Firewalls

Aki Nordlund

aki.nordlund@hut.fi

Agenda

- Cisco PIX firewall product family
- PIX as a network component
- ASA (Adaptive Security Algorithm)
- Network topologies
- Other appliances

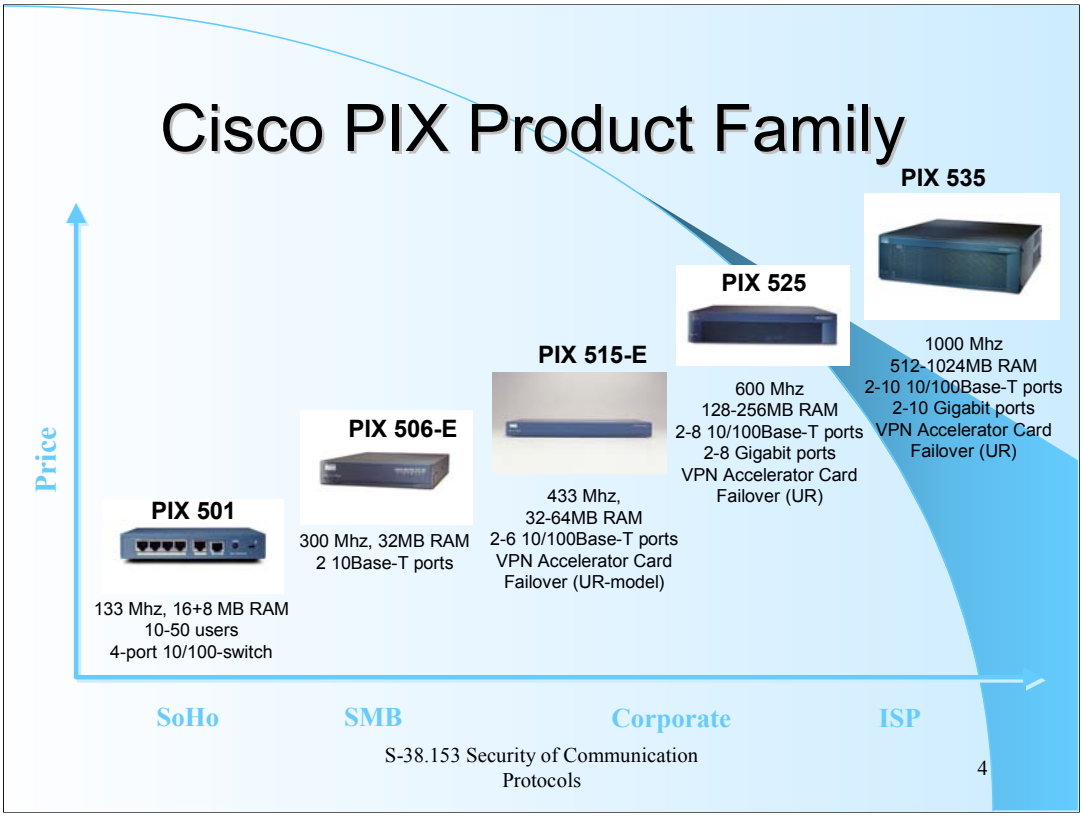
Cisco PIX Firewall

Cisco PIX 500 Series Firewalls are purpose-built security appliances that deliver unprecedented levels of security, performance and reliability.

These platforms provide robust, enterprise-class security services including stateful inspection firewalling, standards-based IPsec Virtual Private Networking (VPN),

intrusion protection and much more in effecective, easy to deploy solutions.

Cisco PIX 500 Firewall Series consists of five models ranging from compact, plug-n-play desktop firewalls for small/home offices to carrier class gigabit firewalls for the most demanding enterprise and service provider environments.



PIX 501

Rather cheap, about 700 €

PIX 501 is targeted for home users or very small offices. It's a good add-on for an ADSL connection. The licensing is based on simultaneous IP addresses used on the protected inside network.

PIX 506E

Affordable, yet very compact packet with features. Based on PIX 515.
Designed for small-and-medium-sized businesses and simple environments.

It will only support environments having two security levels, the inside and outside. This means that a possible dmz-area has to be protected solely by a perimeter router.

Limitations:

-No failover

-32 MB RAM

-Only 10 Mbit/s Ethernet-ports

Cisco PIX 515E

- Operating principle
  - Adaptive Security Algorithm
  - Cut-through proxy
- High performance
  - Max. 100 000 simultaneous connections
  - Max. 3500 new connections/sec
- VPN Accelerator Card (VAC)
- Two licencing alternatives

PIX Firewalls operate using a principle called Adaptive Security Algorithm, ASA. It ensures high performance and secure transactions. PIX515 has also cut-through proxy quality for http and ftp. It will intercept connection attempts to authenticate users, but will cut-through the connection after authentication. This ensures higher throughput than continual proxying function.

The 515E model supports up to 100000 simultaneous sessions through it and the rate of new sessions per second can be as high as 3500.

PIX 515E comes with two licencing alternatives:

-Restricted

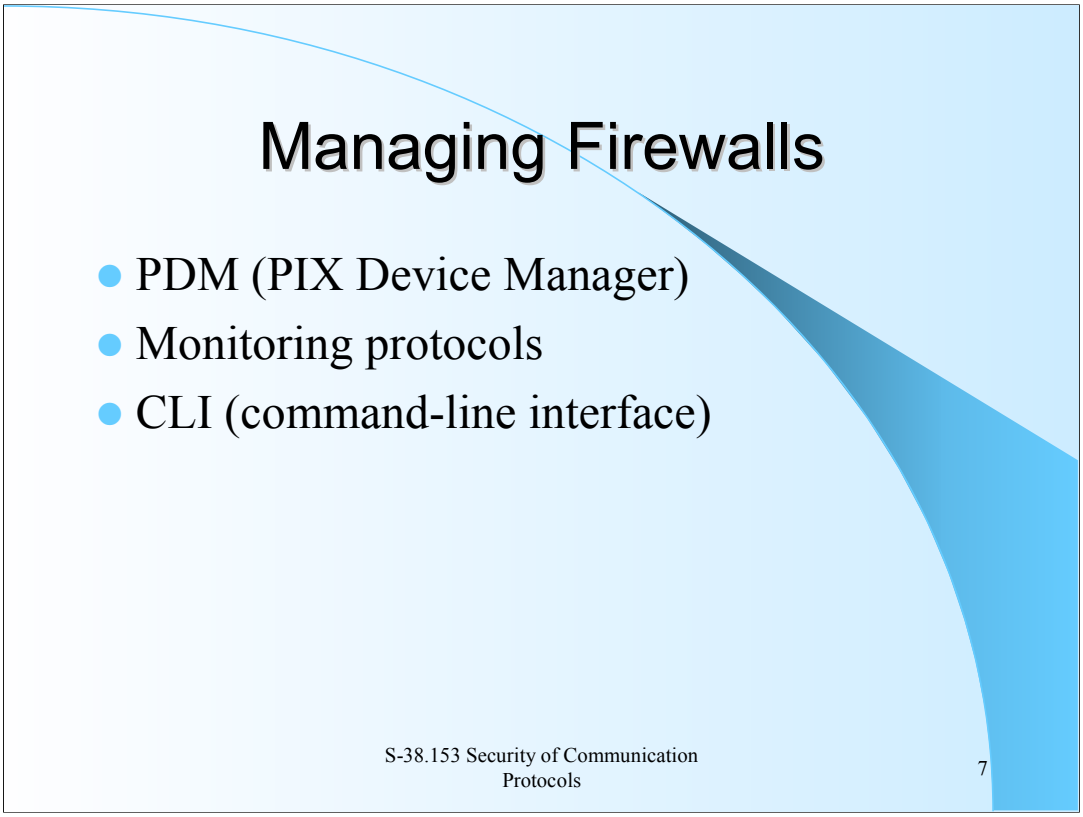
-Unrestricted, which supports morer RAM, more Ethernet ports, VAC and Failover

The VPN accelerator card will triple the VPN tunneling perfomance

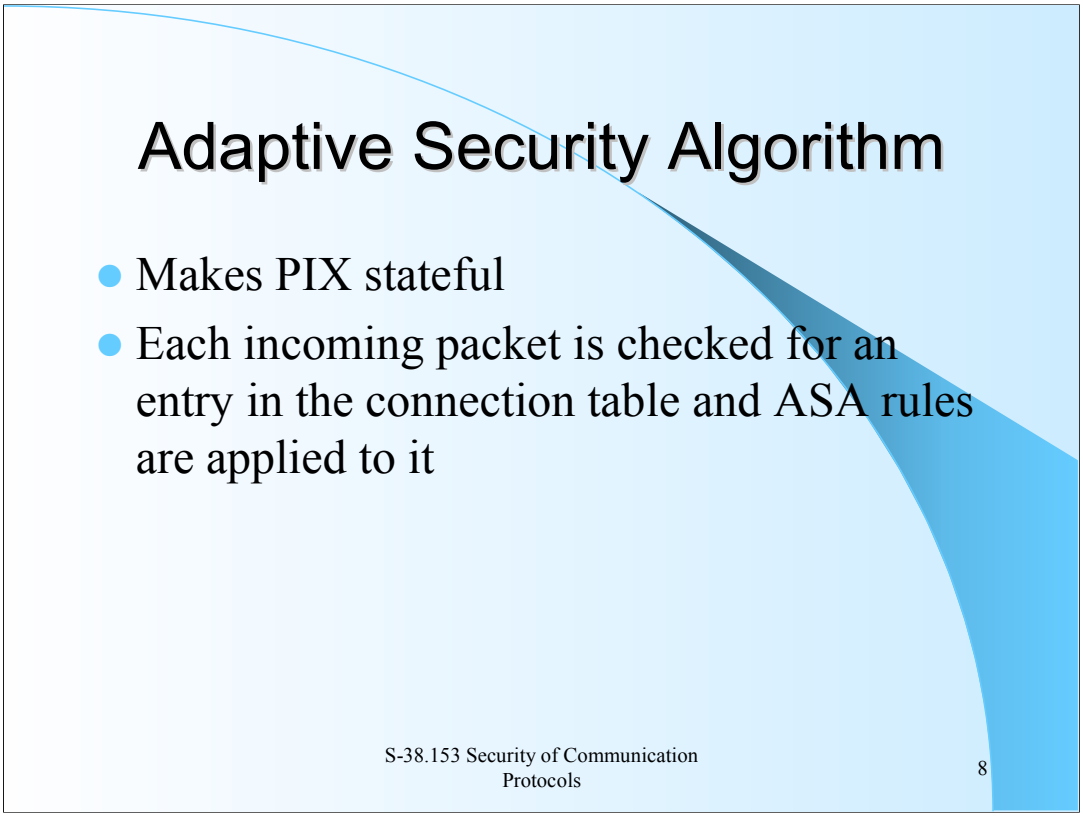
Hardware of a typical firewall on a corporate sized network

PIX 515E-R / PIX 515E-UR*	
Processor:	433 MHz Intel Celeron
Memory:	32MB SDRAM (max. 64 MB*)
Ethernet:	Min. 2 , max. 6 * 10/100 Fast Ethernet
Flash:	16 MB
Performance:	Max. 120000 simultaneous connections 180 Mbps (cleartext), 22 Mbps (3 DES), 63 Mbps (3 DES, VAC)*

PIX 525-R / PIX 525-UR*	
Processor:	600 MHz Intel Pentium III
Memory:	128 MB SDRAM (max. 256 MB*)
Ethernet:	Min. 2, max. 8* 10/100 FastEthernet
Other Media:	Gigabit Ethernet*
Flash:	16 MB
Performance:	Max. 280000* simultaneous connections 370 Mbps (cleartext), 35 Mbps (3 DES), 63 Mbps (3 DES, VAC)*



Administrators can choose from a wide variety of solutions for remotely configuring, monitoring and troubleshooting PIX firewalls. These solutions range from an integrated, Web-based management interface (PIX Device Manager) to centralized, policy-based management tools to support for remote monitoring protocols such as Simple Network Management Protocol (SNMP) and syslog. Administrators can also manage PIX firewalls using a convenient command-line interface (CLI) through a variety of methods including Telnet, Secure Shell (SSH) and an out-of-band console port.



Adaptive Security Algorithm is the basis on which the PIX firewall operates. It's a statetul packet inspection engine that also implements an intuitive security rule system.

Stateful firewall does – as the name implies – care about the state of the data connection. This means that it does not only look for source and destination IP addresses/port numbers but it also tries to understand, in what state the connection is in. Depending on the implementation, stateful firewall might look at state issues on OSI model layers three and four or include also layer 7 (application) information into the rule base.

Generally, stateful firewalls work as follows:

1) A packet enters the firewall.

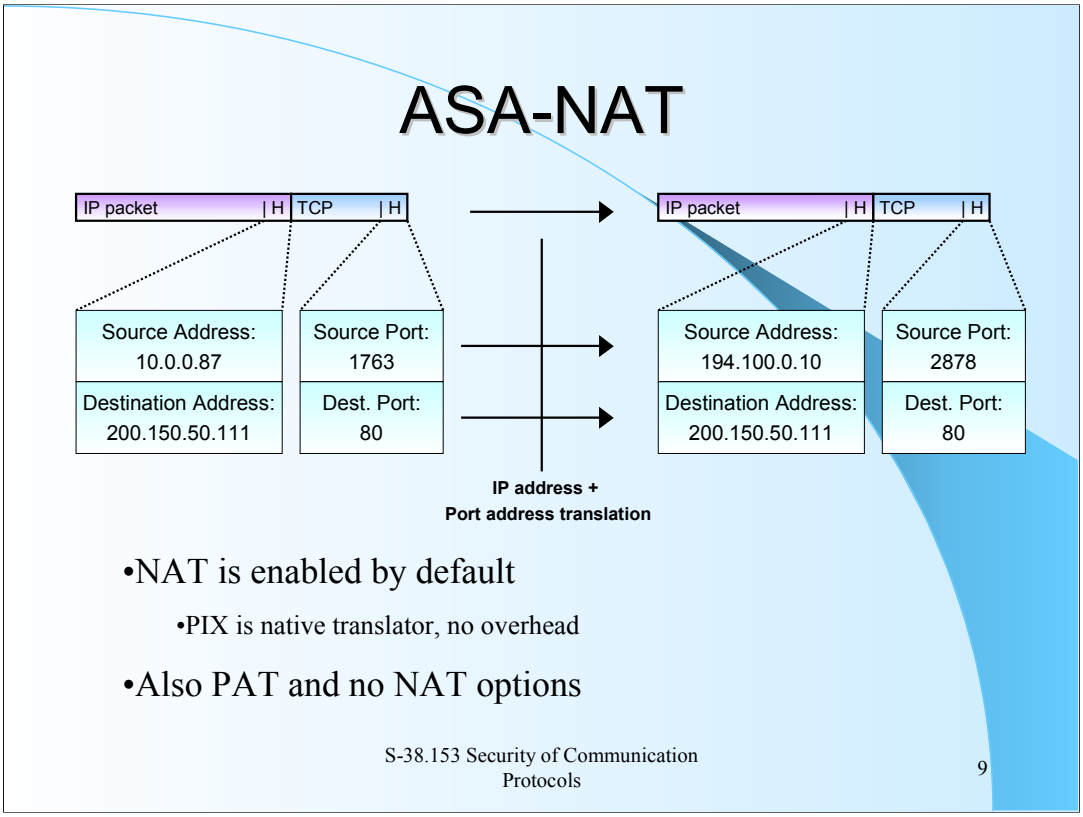
2) State table is consulted, trying to find a flow to which this packet belongs to. If a flow with a suitable state is found, packet is forwarded.

3) If state is not found, packet is examined against the rule base. If allow statement is found, state is created and packet is forwarded. If not, packet is thrown away.

4) State entries time out eventually, if nothing happens an the protocol state level.

The ASA and connection tables ensure security. PIX will do the following for every incoming packet.

- A packet that has no matching entry in the connection table and no embryonic state to it, is automatically rejected.
- All outbound packets are permitted by default. An outbound packet



Extended translation means that in addition to the IP address translation, also the TCP/UDP port numbers are translated. The reason for this to happen is that the inside global address pool is so small that all the inside hosts cannot have an address of their own. Therefore, in order for the hosts to communicate to the outside world, they must use the same inside global address. And to separate the connetions (IP flows), the NAT device uses TCP/UDP port numbers as an identifier.

In the example above, the leftmost network is again the inside network. Let´s assume that a host there wants to speak with a host in the rightmost network. It sends a packet with the header field values as follows:

• IP source address 10.0.0.87, IP destination address 200.150.50.111

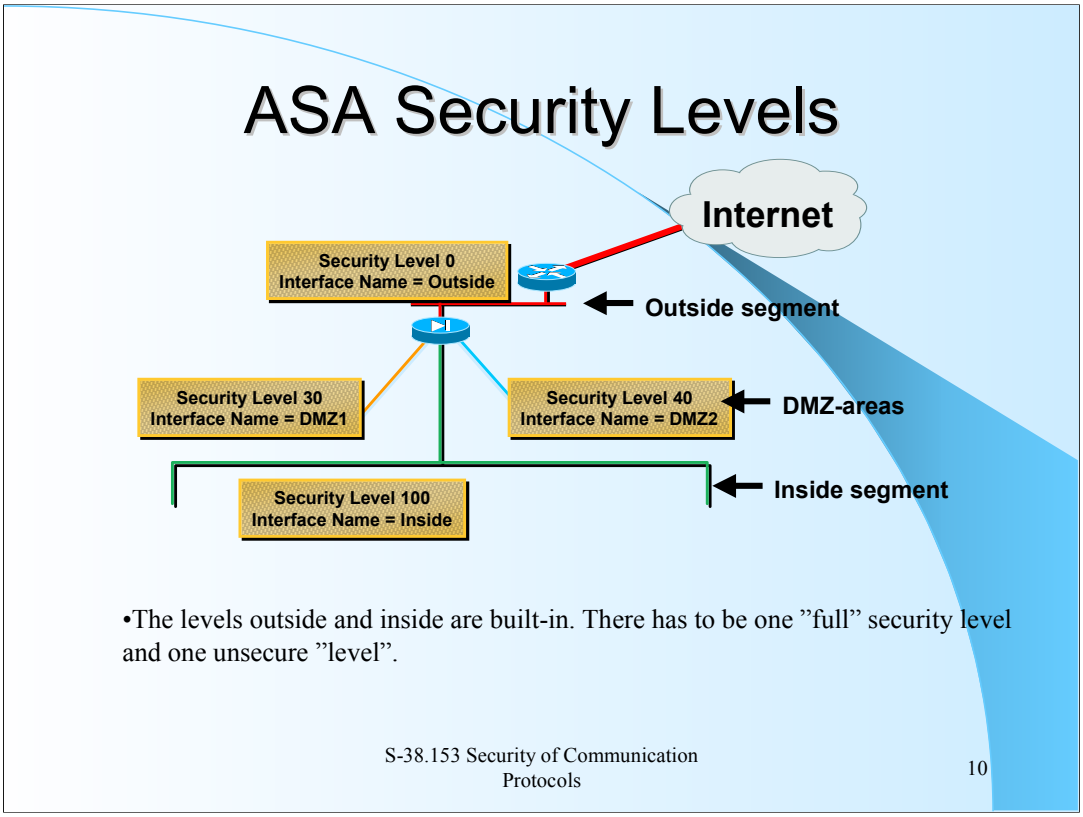
• TCP source port 1763, TCP destination port 80

Now, if the NAT device is configured for NAPT (Network Address Port Translation), then it changes the IP addresses and port numbers. Again, what is actually changed might vary but at least the source address and TCP port will change. In example the administartor could also configure so that the destination address will change. The new parameters for the outgoing packet are:

• IP source address 194.100.0.10, IP destination address 200.150.50.111

• TCP source port 2878, TCP destination port 80

As in the previous example the same will happen vice versa for the incoming packet.



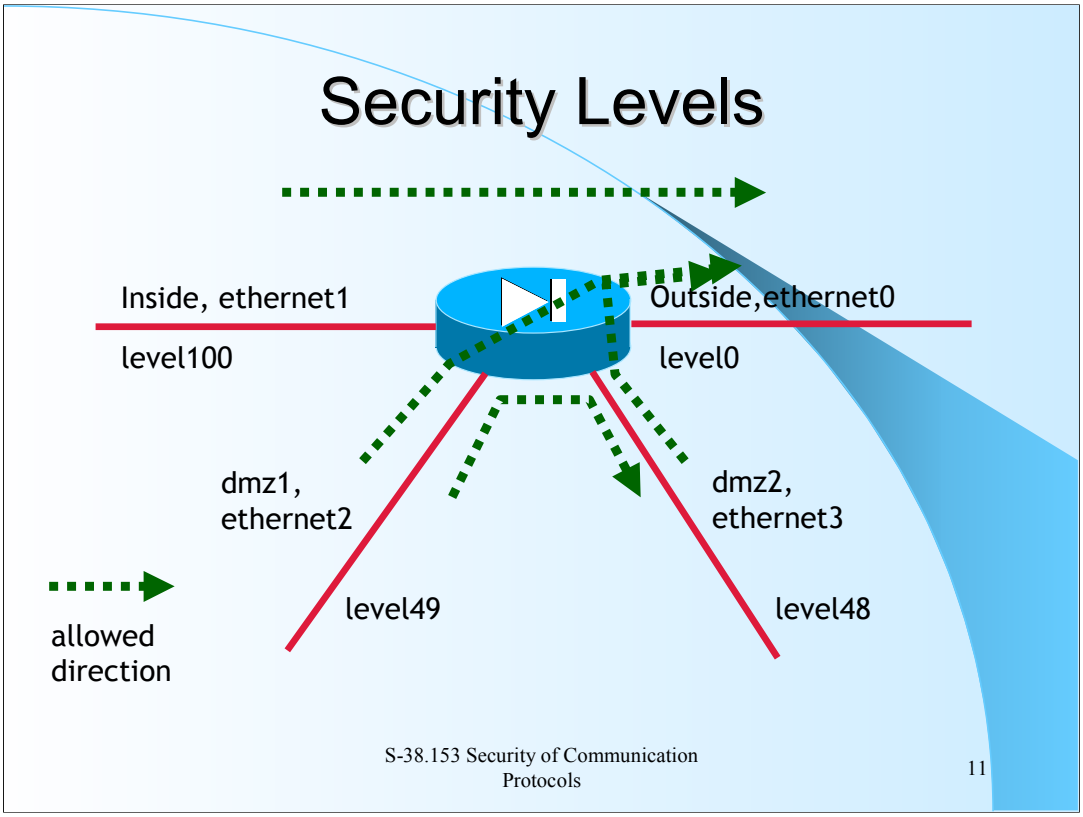
ASA attaches a security value to each interface. If you look at an empty PIX's configuration, you'll notice that two interfaces have built-in security levels:

In the 515E model ethernet0 has security level 0

ethernet1 interface has security level 100

These two levels are always required. In latest software one can assign other physical interfaces these levels, but the two levels have to present in a PIX.

All other interfaces can have security values between 10 and 90.



Although the current PIX can have at max. 8 dmz interfaces whose security levels are between 10 and 90 any two interfaces cannot have the same security level. Security levels can be thought of as water hights. Water will flow from higher to lower level just like traffic through the PIX.

Remember, that Adaptive Security Algorithm makes comparisons of fields in tcp/udp headers and ip headers of an incoming packet with two different tables. A match for a packet coming from a lower security level towards a higher security level has to exist in both the translation table and the connection table.

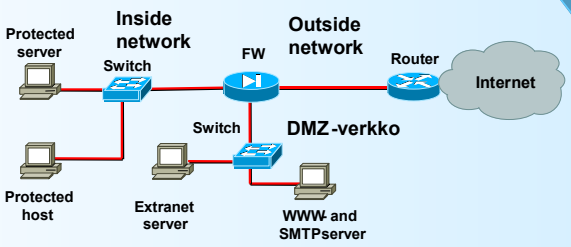
Usually there are services that need to be accessible globally on the dmz, like www, mail, dns. By default, all new connections originating behind the outside interface are denied. For a packet to be able to go from lower to higher security level there needs to be an existing connection in the connection table and, of course, there can't be one since we're talking about a new connection.

The way to circumvent ASA connection table is defining exceptions to ASA. This is done by using access-lists. Access-lists allow all specified traffic through the interface they are attached to, regardless of there being an existing connection in the connection table or not.

The public hosts need to be visible to the public, have a global ip address, either statically defined by PIX or non-translated global ip addresses for the hosts.

Basic Topology

•This represent a generic method of connecting a firewall to a network



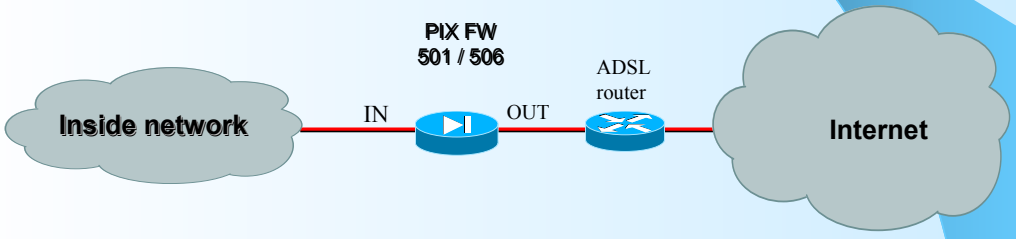
The firewall needs to have a default gateway, just like any host. Firewall is not a router. In addition to having routing information, the perimeter router protects firewall itself from attacks and can weed out the most obvious attack attempts.

If the public hosts would be on the inside, one would have to create ”holes” in the security level rules. By default, nothing flows (uninitiated) from outside to inside, but putting www-servers or smtp-servers there would necessitate access directly to the protected network.

If someone found a security vulnerability in those services and installed a root kit to gain control of those servers, he could attack the rest of the network. The firewall can’t help anymore, since all the traffic would be inside the protected network.

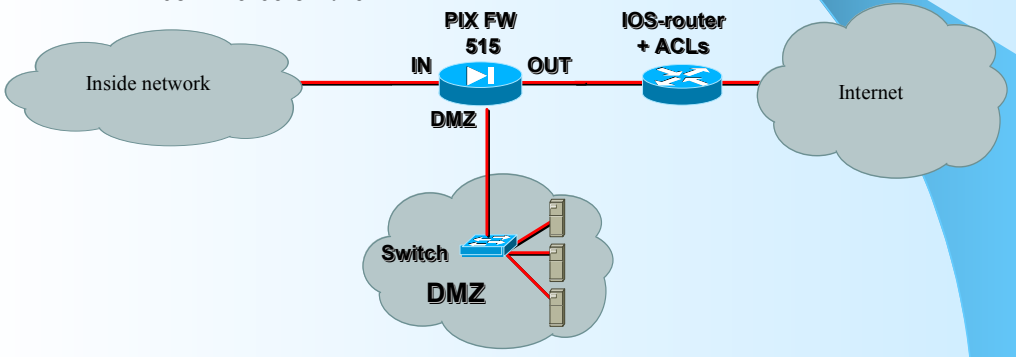
SoHo Topology

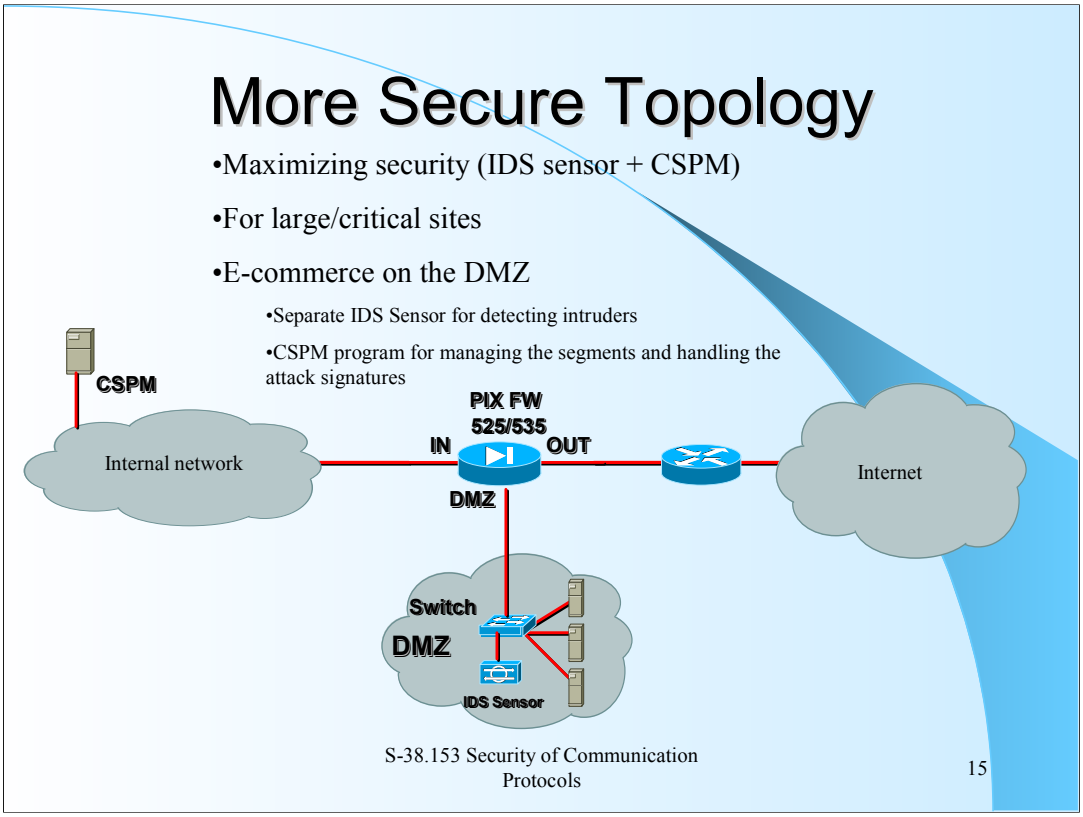
- Small office/Home office
- Firewall protects only inside network
- ISP router's access-list protect ADSL router



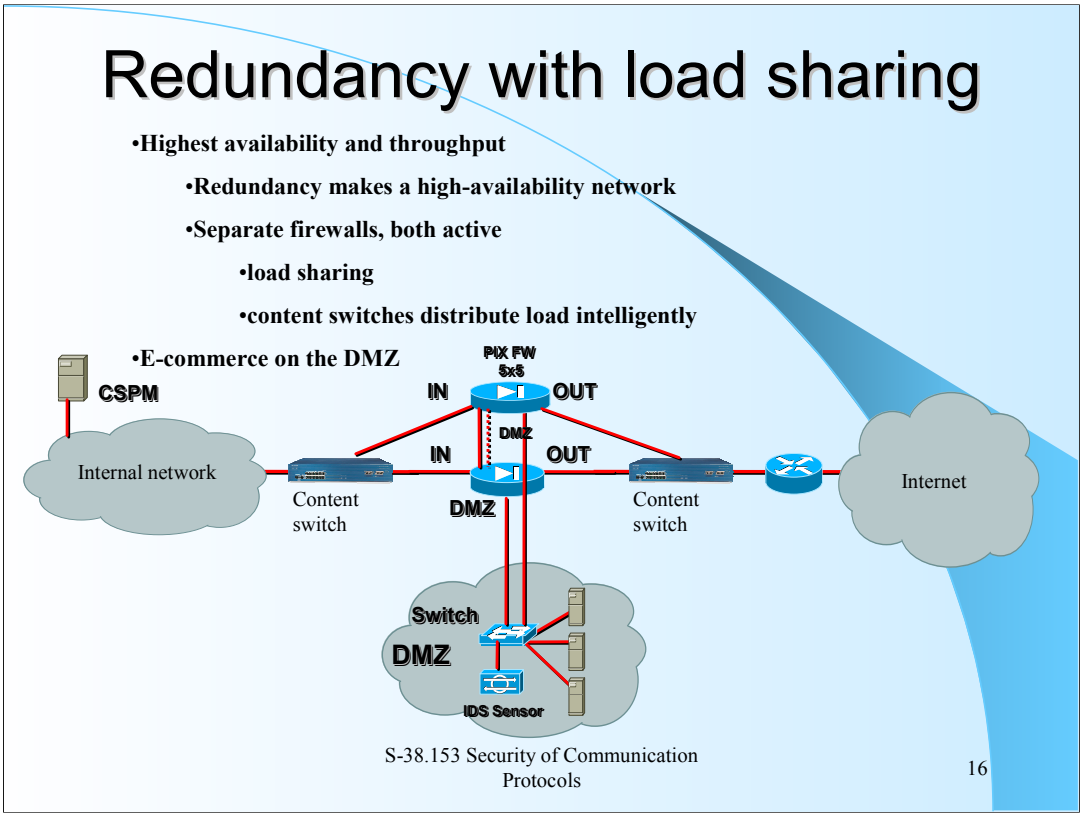
MB Topology

- Medium- sized businesses
- Network is protected by the PIX
- ISP router acl:s provide basic protection
- E-commerce on the DMZ

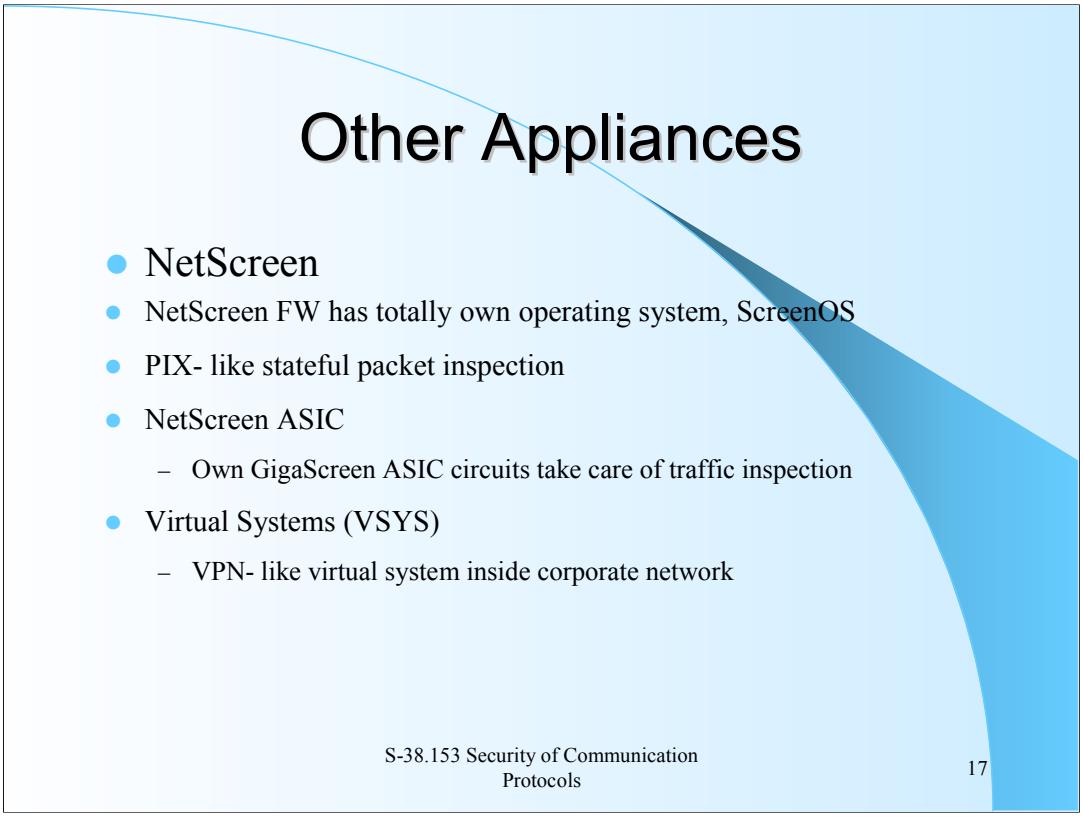




CSPM is short for Cisco Secure Policy Manager. It contains a database of typical attack signatures against which all captured packets are evaluated. It also contains script generators for generating configurations for routers and PIX firewalls, so its also a Manager.



WITHOUT content switches and load-sharing one firewall is active and the other is backup. If active firewall fails, stateful failover happens. Stateful failover means that the backup firewall maintains the same connection and translation table as the primary one. When and if the primary fails, the failover unit has enough information to just keep on relaying traffic.



NetScreen security appliances offer first a solution that integrates firewall, IPSec VPN, and traffic management functionality on NetScreen's custom operating system, ScreenOS. To accelerate this, the NetScreen takes advantage of NetScreen's GigaScreen ASIC for hardware-based acceleration.

Other Appliances

- Nokia IP/Check Point
- Nokia IP platform with Check Point software license
- Two different solution with own management
- Complex and expencive

- SonicWALL
- SonicWALL offers a wide range of low- end products
- Designed to increase security by reducing complexity

Thank you!

Hauskaa Wappua!!