BTNS Core

Michael Richardson (mcr@xelerance.com)
Nico Williams (nicolas.williams@sun.com)

Setup for the examples

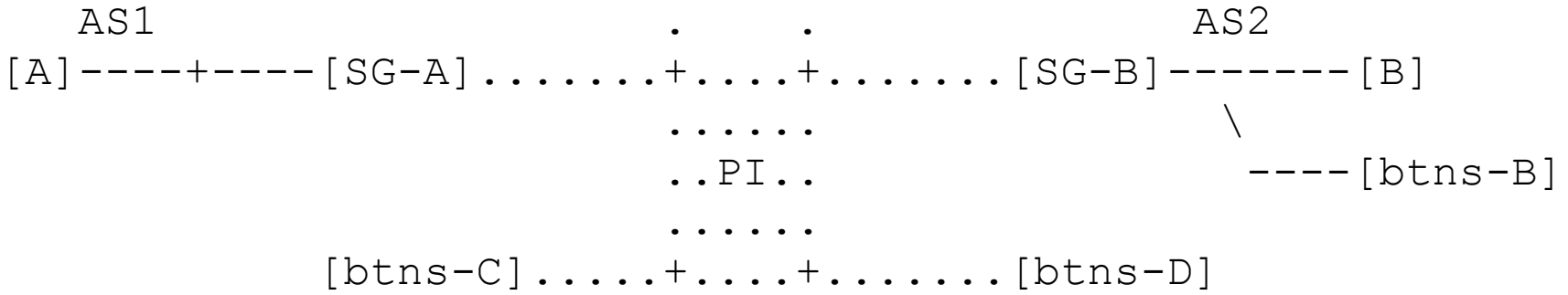

Figure 1: Reference Network Diagram

In this diagram, there are six end-nodes: A, B, C and D. Two of the systems are security gateways: SG-A, SG-B, protecting networks on which [A] and [B] reside. There is a node [Q] which is IPsec and BTNS capable, and node [R] is a simple node, with no IPsec or BTNS capability. Nodes [C] and [D] are BTNS capable. We will examine interactions between the BTNS enabled nodes, and the IPsec enabled nodes.

Nodes C and Q have a fixed addresses. Node D non-fixed addresses.

PI is the Public Internet ("The Wild").

Example #1: sgA

The machine that we will care about will be [SG-A], a firewall device of some kind which we wish to configure to respond to BTNS connections from [C].

Rule	Remote ID	Child SA IDs allowed	SPD Search by
1	<B's ID>	<B's network>	ID
2	<Q's ID>	<Q's host>	ID
3	PUBLICKEY:any	ANY	by-IP

Figure 2: SG-A PAD table

Example #1: sgA

Rule	Local ID/TS	Remote ID/TS	Next Layer Protocol	BTNS ok	Action
1	ID:A	ID:R	ANY	N/A	BYPASS
2	ID:A	ID:Q	ANY	no	PROTECT(ESP,tunnel,AES, SHA256)
3	ID:A	ID:B	ANY	no	PROTECT(ESP,tunnel,AES, SHA256)
4	IP:A-net	IP:ANY	ANY	yes	PROTECT(ESP,transport, integr+conf)

Figure 3: SG-A SPD table

Example #2: Q

Rule	Remote ID	IDs allowed	SPD Search by
1	<A's ID>	<A's address>	ID
2	PUBLICKEY:any	ANY	by-IP

Figure 4: Q PAD table

Rule	Local ID/TS	Remote ID/TS	Next Layer Protocol	BTNS ok	Action
1	ID:Q	ID:A	ANY	no	PROTECT(ESP,tunnel,AES, SHA256)
2	IP:Q	IP:ANY and port 2049	ANY	yes	PROTECT(ESP,transport, integr+conf)

Figure 5: SG-A SPD table

Example #3: C

Rule	Remote ID	Child SA IDs allowed	SPD Search by
1	PUBLICKEY:any	ANY	by-IP

Figure 6: Q PAD table

Rule	Local ID/TS	Remote ID/TS	Next Layer Protocol	BTNS ok	Action
1	IP:C	IP:ANY and port 2049	ANY	yes	PROTECT(ESP,transport, integr+conf)
2	ID:C	IP:ANY	ANY	N/A	BYPASS

Figure 7: SG-A SPD table